Last Revised: June 22, 2016

**Policy 1: General HIPAA Compliance Policy**

**Introduction**

**PROVIDER COMPLIANCE SOLUTIONS** has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act “ARRA”) and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

**PROVIDER COMPLIANCE SOLUTIONS** hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information (“IIHI”) generally, and Protected Health Information (“PHI”) as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

This applies to all Policies in this program.

**Scope of Policy**

This policy governs General HIPAA Compliance for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to become and to remain in full compliance with all the requirements of HIPAA.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
* All HIPAA compliance-related documentation will be managed and maintained for a minimum of six (6) years from the date of creation or last revision, whichever is later, in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Document Retention policy.

**Procedures**

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **PROVIDER COMPLIANCE SOLUTIONS** commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

* **Privacy Policies and Procedures** -- **PROVIDER COMPLIANCE SOLUTIONS** shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.
* **Privacy Personnel** -- **PROVIDER COMPLIANCE SOLUTIONS** shall designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on **PROVIDER COMPLIANCE SOLUTIONS**’s privacy practices.
* **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the **PROVIDER COMPLIANCE SOLUTIONS** (whether or not they are paid by **PROVIDER COMPLIANCE SOLUTIONS**). **PROVIDER COMPLIANCE SOLUTIONS** shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.
* **Sanctions** -- **PROVIDER COMPLIANCE SOLUTIONS** shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA’s Privacy and Security Rules.
* **Mitigation** -- **PROVIDER COMPLIANCE SOLUTIONS** shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
* **Data Safeguards** -- **PROVIDER COMPLIANCE SOLUTIONS** shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
* **Complaints** -- **PROVIDER COMPLIANCE SOLUTIONS** shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **PROVIDER COMPLIANCE SOLUTIONS** shall explain those procedures in its privacy practices notice.
* **Retaliation and Waiver** -- **PROVIDER COMPLIANCE SOLUTIONS** shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **PROVIDER COMPLIANCE SOLUTIONS** shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.
* **Documentation and Record Retention** -- **PROVIDER COMPLIANCE SOLUTIONS** shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

**Compliance and Enforcement**

All **PROVIDER COMPLIANCE SOLUTIONS** managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013General Rules for Uses and Disclosures of Protected Health Information: Use and Disclosure for Treatment, Payment and Health Care Operations - § 164.502(a)**  |

*Standard*. A PROVIDER COMPLIANCE SOLUTIONS or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

1. *Covered entities: Permitted uses and disclosures*. A PROVIDER COMPLIANCE SOLUTIONS is permitted to use or disclose protected health information as follows:
	1. To the individual;
	2. For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
	3. Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the PROVIDER COMPLIANCE SOLUTIONS has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
	4. Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;
	5. Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
	6. As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).
2. *Covered entities: Required disclosures*. A PROVIDER COMPLIANCE SOLUTIONS is required to disclose protected health information:
	1. To an individual, when requested under, and required by § 164.524 or § 164.528; and
	2. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the PROVIDER COMPLIANCE SOLUTIONS's compliance with this subchapter.
3. *Business associates: Permitted uses and disclosures*. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the PROVIDER COMPLIANCE SOLUTIONS, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.
4. *Business associates: Required uses and disclosures*. A business associate is required to disclose protected health information:
	1. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.
	2. To the PROVIDER COMPLIANCE SOLUTIONS, individual, or individual's designee, as necessary to satisfy a PROVIDER COMPLIANCE SOLUTIONS's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.
5. *Prohibited uses and disclosures*.
	1. *Use and disclosure of genetic information for underwriting purposes*:

Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

* + 1. Except as provided in paragraph (a)(5)(i)(B) of this section:
			1. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
			2. The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
			3. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
			4. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
		2. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.
	1. *Sale of protected health information*:
		1. Except pursuant to and in compliance with § 164.508(a)(4), a PROVIDER COMPLIANCE SOLUTIONS or business associate may not sell protected health information.
		2. For purposes of this paragraph, sale of protected health information means:
			1. Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a PROVIDER COMPLIANCE SOLUTIONS or business associate, if applicable, where the PROVIDER COMPLIANCE SOLUTIONS or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.
			2. Sale of protected health information does not include a disclosure of protected health information:
			3. For public health purposes pursuant to § 164.512(b) or § 164.514(e)
			4. For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the PROVIDER COMPLIANCE SOLUTIONS or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;
			5. For treatment and payment purposes pursuant to § 164.506(a);
			6. For the sale, transfer, merger, or consolidation of all or part of the PROVIDER COMPLIANCE SOLUTIONS and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);
			7. To or by a business associate for activities that the business associate undertakes on behalf of a PROVIDER COMPLIANCE SOLUTIONS, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the PROVIDER COMPLIANCE SOLUTIONS to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;
			8. To an individual, when requested under § 164.524 or § 164.528;
			9. Required by law as permitted under § 164.512(a); and
			10. For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the PROVIDER COMPLIANCE SOLUTIONS or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: General Rules - § 164.306** |

1. *General requirements*. Covered entities and business associates must do the following:
	1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the PROVIDER COMPLIANCE SOLUTIONS or business associate creates, receives, maintains, or transmits.
	2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
	3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
	4. Ensure compliance with this subpart by its workforce.
2. *Flexibility of approach*.
	1. Covered entities and business associates may use any security measures that allow the PROVIDER COMPLIANCE SOLUTIONS or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
	2. In deciding which security measures to use, a PROVIDER COMPLIANCE SOLUTIONS or business associate must take into account the following factors:
		1. The size, complexity, and capabilities of the PROVIDER COMPLIANCE SOLUTIONS or business associate.
		2. The PROVIDER COMPLIANCE SOLUTIONS's or the business associate's technical infrastructure, hardware, and software security capabilities.
		3. The costs of security measures.
		4. The probability and criticality of potential risks to electronic protected health information.
3. *Standards*. A PROVIDER COMPLIANCE SOLUTIONS or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.
4. *Implementation specifications*. In this subpart:
	1. Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.
	2. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a PROVIDER COMPLIANCE SOLUTIONS or business associate must implement the implementation specifications.
	3. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a PROVIDER COMPLIANCE SOLUTIONS or business associate must--
		1. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
		2. As applicable to the PROVIDER COMPLIANCE SOLUTIONS or business associate--
			1. Implement the implementation specification if reasonable and appropriate; or
			2. If implementing the implementation specification is not reasonable and appropriate--
				1. Document why it would not be reasonable and appropriate to implement the implementation specification; and
				2. Implement an equivalent alternative measure if reasonable and appropriate.
5. *Maintenance*. A PROVIDER COMPLIANCE SOLUTIONS or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii).

|  |
| --- |
| **HHS Regulations as Amended January 2013Compliance and Enforcement: Responsibilities of Covered Entities - § 160.310** |

1. *Provide records and compliance reports*. A PROVIDER COMPLIANCE SOLUTIONS or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the PROVIDER COMPLIANCE SOLUTIONS or business associate has complied or is complying with the applicable administrative simplification provisions.
2. *Cooperate with complaint investigations and compliance reviews*. A PROVIDER COMPLIANCE SOLUTIONS or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the PROVIDER COMPLIANCE SOLUTIONS or business associate to determine whether it is complying with the applicable administrative simplification provisions.
3. *Permit access to information*.
	1. A PROVIDER COMPLIANCE SOLUTIONS or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a PROVIDER COMPLIANCE SOLUTIONS or business associate must permit access by the Secretary at any time and without notice.
	2. If any information required of a PROVIDER COMPLIANCE SOLUTIONS or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the PROVIDER COMPLIANCE SOLUTIONS or business associate must so certify and set forth what efforts it has made to obtain the information.
	3. Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 2: Policies and Procedures Policy**

**Scope of Policy**

This policy governs the establishment and maintenance of policies and procedures for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a covered entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to create and implement appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics.
* All policies and procedures shall be updated and amended as needed or as required by law.
* All policies and procedures shall be distributed to, or made otherwise available to, the entire workforce.
* All policies and procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
* All members of the workforce are required to read, understand, and comply with this and all other policies and procedures created and implemented by **PROVIDER COMPLIANCE SOLUTIONS**.

**Procedures**

* **PROVIDER COMPLIANCE SOLUTIONS** shall create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA Rules and Regulations as well as with applicable State laws and statutes.
* **PROVIDER COMPLIANCE SOLUTIONS** shall designate a qualified individual to assume control of the policies and procedures process. This individual shall report to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and shall execute the creation or revision process in a timely manner, in order to meet the current HIPAA Compliance Deadline of September 23, 2013.
* **PROVIDER COMPLIANCE SOLUTIONS** shall engage its qualified legal counsel to guide or review the policies and procedures creation/revision process, and to intercede where necessary, to ensure **PROVIDER COMPLIANCE SOLUTIONS**’s policies and procedures meet all applicable HIPAA (and other) standards.
* **PROVIDER COMPLIANCE SOLUTIONS** shall internally publish its HIPAA policies and procedures, when complete, to its workforce members, and shall provide appropriate training to members of its workforce on the interpretation and implementation of its policies and procedures.
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

---------------------------------------------------------------------------------------------------------------------

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Policies and Procedures and Documentation Requirements - § 164.316** |

A Provider Compliance Solutions or business associate must, in accordance with § 164.306:

1. *Standard: Policies and procedures*. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A Provider Compliance Solutions or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
	1. *Standard: Documentation*.
		1. Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
		2. If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
	2. *Implementation specifications*:
		1. *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
		2. *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
		3. *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 3: HIPAA Documentation Policy**

**Scope of Policy**

This policy governs the creation and maintenance of HIPAA-related documentation for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for **PROVIDER COMPLIANCE SOLUTIONS** must document all HIPAA-related activities that require documentation.
* All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.
* Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by **PROVIDER COMPLIANCE SOLUTIONS**.
* All HIPAA-related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by **PROVIDER COMPLIANCE SOLUTIONS**.
* All required HIPAA documentation shall be securely and appropriately maintained and stored in accordance with HIPAA Regulations and with **PROVIDER COMPLIANCE SOLUTIONS**’s policy on document retention.
* HIPAA documentation shall be made available, as needed, to all workforce members who are authorized to access it, and shall be made available to appropriate authorities for audits, investigations, and other purposes authorized or required by law.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:**

• Maintain written or electronic copies of communications that the Rules require to be in writing.

• Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.

• Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.

Note: The six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 4: HIPAA Documentation Retention Policy**

**Scope of Policy**

This policy governs HIPAA Documentation Retention for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.
* HIPAA documentation shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
* HIPAA documentation shall be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards.

**Procedures**

* Documents older than 6 years will be destroyed by HIPAA complaint documentation destruction company.
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:**

• Maintain written or electronic copies of communications that the Rules require to be in writing.

• Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.

• Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.

Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 4: HIPAA Documentation Retention Policy**

**Scope of Policy**

This policy governs HIPAA Documentation Retention for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.
* HIPAA documentation shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
* HIPAA documentation shall be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:**

• Maintain written or electronic copies of communications that the Rules require to be in writing.

• Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.

• Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.

Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 5: HIPAA Documentation Availability Policy**

**Scope of Policy**

This policy governs HIPAA Documentation Availability for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations concerned with the availability of HIPAA-related documentation, in accordance with the HIPAA requirements at § 164.310, § 164.316, and § 164.530(j), among others.
* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to make all HIPAA-related documentation available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains.
* All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation, or who require such documentation in the performance of their work-related duties.
* Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
* No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

**Procedures**

* Provider Compliance Solutions will make the HIPAA compliance program available to the Security Risk Officer and to all staff members.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:**

• Maintain written or electronic copies of communications that the Rules require to be in writing.

• Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.

• Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.

Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

**HIPAA Documentation includes the following:**

* HIPAA Policies and Procedures.
* HIPAA Risk Analysis and related notes and research materials
* Policies and Procedures for minimum necessary uses by your work force.
* Accounting documentation which includes…
* information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures; description, etc.);
* the written accounting that is provided to the individual; and
* the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals
* Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
* All complaints received and their disposition, if any.
* All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.
* The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
* Training provided (i.e., topics, dates, and, ideally, participants).
* Sanctions imposed against non-complying work force members.
* All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
* The methods and results of analyses that justify release of de-identified information.
* Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.
* Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
* The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
* All signed authorizations and revocations.
* All approved confidential communication requests and terminations or revocations.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 6: HIPAA Documentation Updating Policy**

**Scope of Policy**

This policy governs HIPAA Documentation Updating for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
* Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.
* Reviews of HIPAA-related documentation shall be made periodically, but at least every \_\_\_\_\_ months for the purposes of this policy.
* Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be made by **PROVIDER COMPLIANCE SOLUTIONS**’s designated Privacy Officer or HIPAA Officer.
* Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be documented according to **PROVIDER COMPLIANCE SOLUTIONS**’s Documentation Policy.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Rules require that Covered Entities maintain their policies and procedures in written or electronic form, as well as the following:**

• Maintain written or electronic copies of communications that the Rules require to be in writing.

• Maintain written or electronic records of actions, activities, or designations the Rules require to be documented.

• Regulated entities must retain all documentation required by the Regulations for six years from the date of its creation or six years from the date when it last was in effect, whichever is later.

Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.

**HIPAA Documentation includes the following:**

* HIPAA Policies and Procedures.
* HIPAA Risk Analysis and related notes and research materials
* Policies and Procedures for minimum necessary uses by your work force.
* Accounting documentation which includes…
* information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures, description, etc.);
* the written accounting that is provided to the individual; and
* the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
* Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
* All complaints received and their disposition, if any.
* All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions, and terminations.
* The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
* Training provided (i.e., topics, dates, and, ideally, participants).
* Sanctions imposed against non-complying work force members.
* All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
* The methods and results of analyses that justify release of de-identified information.
* Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.
* Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
* The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
* All signed authorizations and revocations.
* All approved confidential communication requests and terminations or revocations.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 7: HIPAA Investigations Policy**

**Scope of Policy**

This policy governs HIPAA Investigations for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* **PROVIDER COMPLIANCE SOLUTIONS** recognizes that the U.S. Department of Health and Human Services (“HHS”), its Office for Civil Rights (“OCR”) and other designees, as well as State Attorneys General, are all authorized and empowered to investigate Covered Entities and Business Associates in matters of HIPAA compliance and enforcement.
* **PROVIDER COMPLIANCE SOLUTIONS** recognizes that timely and full cooperation with such investigative bodies is mandatory under HIPAA law; and that failure to cooperate with any HIPAA investigation is itself a violation of HIPAA Rules.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to not impede or obstruct any HIPAA-related investigations conducted by HHS.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

**Procedures**

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

* Whenever a HHS investigation is discovered, the following persons must be immediately notified:
	+ Attorneys (HIPAA counsel and local counsel, if different)
	+ Executive Management
	+ Privacy Officer
	+ Security Officer
	+ Compliance Officer
	+ Health Information Management Department and/or the Custodian of Records
	+ Cooperate, but do not volunteer information or records that are not requested.
	+ Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. BE SURE that you’ve made appropriate requests for I.D. and that they’ve been unreasonably refused before you do.)
	+ Have at least one, if not two witnesses available to testify as to your requests and their responses.
	+ Ask for the name and telephone number of the lead investigator’s supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering “hard feelings.” Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
	+ Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask.
	+ Permit the investigators to have access to protected health information (“PHI”), in accordance with our notice of privacy practices (“NPP”), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
	+ Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
	+ Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
	+ Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
	+ Ask the investigators for documents related to the investigation. For example, request:
	+ copies of any search warrants and/or entry and inspection orders
	+ copies of any complaints
	+ a list of patients they are interested in
	+ a list of documents/items seized
	+ Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
	+ Do not leave the investigators alone, if possible. Assign someone to “assist” each investigator present.
	+ Do not offer food (coffee, if already prepared, and water, if already available, is ok. Don’t do anything that could be construed as a “bribe” or a “kickback” to induce favorable treatment, such as offering to buy the investigators lunch.
	+ Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.
	+ < Add specific procedure here >
	+ < Add specific procedure here >
	+ < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

1. Personnel that may be interviewed

• President, CEO or Director

• HIPAA Compliance Officer

• Lead Systems Manager or Director

• Systems Security Officer

• Lead Network Engineer and/or individuals responsible for:

o administration of systems which store, transmit, or access Electronic Protected Health Information (EPHI)

o administration systems networks (wired and wireless)

o monitoring of systems which store, transmit, or access EPHI

o monitoring systems networks (if different from above)

• Computer Hardware Specialist

• Disaster Recovery Specialist or person in charge of data backup

• Facility Access Control Coordinator (physical security)

• Human Resources Representative

• Director of Training

• Incident Response Team Leader

• Others as identified….

2. Documents and other information that may be requested for investigations/reviews

a. Policies and Procedures and other Evidence that Address the Following:

• Prevention, detection, containment, and correction of security violations

• Employee background checks and confidentiality agreements

• Establishing user access for new and existing employees

• List of authentication methods used to identify users authorized to access EPHI

• List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements

• List of software used to manage and control access to the Internet

• Detecting, reporting, and responding to security incidents (if not in the security plan)

• Physical security

• Encryption and decryption of EPHI

• Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)

• Monitoring systems use - authorized and unauthorized

• Use of wireless networks

• Granting, approving, and monitoring systems access (for example, by level, role, and job function)

• Sanctions for workforce members in violation of policies and procedures governing EPHI access or use

• Termination of systems access

• Session termination policies and procedures for inactive computer systems

• Policies and procedures for emergency access to electronic information systems

• Password management policies and procedures

• Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)

• Disposal of media and devices containing EPHI

b. Other Documents:

• Entity-wide Security Plan

• Risk Analysis (most recent)

• Risk Management Plan (addressing risks identified in the Risk Analysis)

• Security violation monitoring reports

• Vulnerability scanning plans

o Results from most recent vulnerability scan

• Network penetration testing policy and procedure

o Results from most recent network penetration test

• List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)

• Configuration standards to include patch management for systems which store, transmit, or access EPHI (including workstations)

• Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI

• Organization chart to include staff members responsible for general HIPAA compliance to include the protection of EPHI

• Examples of training courses or communications delivered to staff members to ensure awareness and understanding of EPHI policies and procedures (security awareness training)

• Policies and procedures governing the use of virus protection software

• Data backup procedures

• Disaster recovery plan

• Disaster recovery test plans and results

• Analysis of information systems, applications, and data groups according to their criticality and sensitivity

• Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain EPHI

• List of all Primary Domain Controllers (PDC) and servers

• Inventory log recording the owner and movement media and devices that contain EPHI

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 8: Breach Notification Policy**

**Scope of Policy**

This policy governs Breach Notification for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
* Compliance with HIPAA’s breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
* Timely notifications to consumers about breaches of individually identifiable health information can help reduce or prevent identity theft and fraud.
* Timely notifications to consumers about breaches of individually identifiable health information can help protect our business and reputation.
* Only breaches of “unsecured” (unencrypted or not destroyed) protected health information trigger HIPAA’s breach notification requirements.

**Definitions**

As used within the HIPAA Final (“Omnibus”) Rule, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

1. Breach excludes:
	1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
	2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
	3. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
	1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
	2. The unauthorized person who used the protected health information or to whom the disclosure was made;
	3. Whether the protected health information was actually acquired or viewed; and
	4. The extent to which the risk to the protected health information has been mitigated.

*Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide timely notifications to affected (patients and/or) consumers about breaches of individually identifiable health information.
* Model breach notification letters or emails shall be developed and prepared to be used as needed.
* **PROVIDER COMPLIANCE SOLUTIONS** shall notify individuals when a reportable breach is discovered. A breach is treated as “discovered” by the **PROVIDER COMPLIANCE SOLUTIONS** the first day on which such breach is known or should reasonably have been known to any employee or agent of **PROVIDER COMPLIANCE SOLUTIONS**, other than the person who committed the breach.
* Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.

**Procedures**

* Breach Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
* First class mail shall be the default method of notification. **PROVIDER COMPLIANCE SOLUTIONS** may use e-mail if requested by the individual, or substitute notice via our website or local print or broadcast media if we do not have current contact information.
* **PROVIDER COMPLIANCE SOLUTIONS** must notify major local media outlets of a breach affecting more than 500 individuals.
* Business Associates of **PROVIDER COMPLIANCE SOLUTIONS** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **PROVIDER COMPLIANCE SOLUTIONS**’s designated HIPAA Officer or Privacy Officer.
* Business Associate contracts, whether existing or new, shall have corresponding breach notification requirements included in them.
* Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.
* All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Documentation Policy.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**NOTES – The material below is for reference purposes only, and does not constitute legal advice. Remove this NOTES section when editing this Policy.**

**General information regarding Breaches and Breach Notification under the Final “Omnibus” HIPAA Rule...**

* The abbreviation “CE” refers to “Covered Entities”.
* The abbreviation “BA” refers to “Business Associates”.

**Under the Omnibus Final Rule**

The Omnibus Rule amends the definition of breach to clarify that the impermissible acquisition, access, use, or disclosure of PHI *is presumed to be a breach* and breach notification is necessary unless a covered entity or business associate can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised.

Under the final rule, CEs must determine whether there is a *low probability* that the PHI was compromised – a far different standard than whether there is a significant risk of harm to the individual. As a result, CEs will have to significantly modify their current procedures for conducting a risk assessment, and it is likely that more impermissible uses and disclosures will be reportable breaches under the Final Rule than under the interim final rule.

The new risk assessment requirement for breaches becomes effective September 23, 2013.

**Four Factors to Consider in a Breach Risk Assessment**

The Omnibus Rule identifies four factors that must be considered in a risk assessment:

1. The nature and extent of the PHI involved -- Was sensitive data, such as Social Security numbers and detailed clinical information, involved in an incident?
2. The unauthorized person who used the PHI or to whom the disclosure was made -- If the disclosures were to another HIPAA-regulated entity or to a federal agency, for example, this may result in a “lower probability that the [PHI] has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.”
3. Whether the PHI actually was acquired or viewed -- This would typically involve a forensic analysis or investigation that could determine whether PHI contained on a lost or stolen laptop or other portable electronic device actually was viewed or accessed.
4. The extent to which the risk to the PHI has been mitigated -- This might involve reaching out to an unauthorized recipient of the PHI to obtain “satisfactory assurances” that any PHI sent to a recipient was not further used or disclosed but instead destroyed.

HHS indicates that covered entities and business associates must evaluate the overall probability that PHI has been compromised by considering all combined factors in a thorough risk assessment. HHS states that it will issue additional guidance in the future to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.

HHS expects risk assessments to be “thorough, completed in good faith, and for the conclusions reached to be reasonable,” and noted “additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised.”

**Breach Notification Only Applies to “Unsecured” PHI**

Breach Notification only applies to PHI that *has not* been “secured” (encrypted) according to HHS and NIST standards. PHI that has been secured by these standards, and is subsequently breached, *does not invoke any Breach Notification requirements*.

The current encryption Standard referenced in the Final Rule is: “*Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*”.

(74 Federal Register, Pages 42,740-42,742)

This Breach Notification exception *does not apply* to paper, film, and other hardcopy PHI, because these materials cannot be electronically encrypted (protected) in their native forms.

**Exceptions to the Definition of “Breach”**

The Interim Final Rule (prior to the Omnibus Final Rule) included three exceptions to the definition of “breach.” These exceptions were adopted without modification in the Final Omnibus Rule. The exceptions are as follows:

1. Unintentional acquisition, access, or use of PHI by an employee or other person acting under the authority of a CE or BA if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the CE or BA, and such information is not further acquired, accessed, used, or disclosed by any person;
2. Inadvertent disclosure of PHI from one person authorized to access PHI at a facility operated by a CE or BA to another person similarly situated at the same facility, and the information received is not further acquired, accessed, used or disclosed without authorization by any person; and
3. Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

**Breaches - Limited Data Set Exception Removed**

The Omnibus Rule removes the exception for limited data sets that do not contain birth dates or ZIP codes. By removing this exception, the Omnibus Rule requires that the impermissible acquisition, access, use, or disclosure of limited data sets, even those that do not contain birth dates or ZIP codes, be subject to a risk assessment to demonstrate that breach notification is not required.

Under the Final Rule, CEs must perform a risk assessment evaluating the required factors, following the impermissible use or disclosure of any limited data set, even if it *excludes* birth dates and zip codes.

**Breaches – Voluntary Notifications Without Risk Assessment**

A CE or BA has the discretion to *voluntarily* provide the required notifications following an impermissible use or disclosure of Protected Health Information *without* performing a risk assessment.

**Breaches -- Notification to HHS**

The HITECH Act requires CEs to notify HHS of breaches of unsecured PHI, with the timing of such notification based on the size of the breach. As has been the case, the Omnibus Rule requires notification of breaches affecting 500 or more individuals contemporaneously with notification of the affected individuals.

For breaches affecting fewer than 500 individuals, the Omnibus Rule clarifies that CEs must notify HHS within 60 days after the end of the calendar year in which the breaches were “discovered,” not in which the breaches “occurred.”

**Breaches – Notifications to Individuals and Media**

The Omnibus Final Rule adopts almost all of the Interim Final Rule’s Breach Notification provisions without modification, including the following:

1. CEs must notify individuals when a reportable breach is discovered. A breach is treated as “discovered” by the CE the first day on which such breach is known or should reasonably have been known to any employee or agent of the CE, other than the person who committed the breach.
2. Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.
3. Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
4. First class mail is the default method of notification. A CE may use e-mail if requested by the individual, or substitute notice via the CE’s website or local print or broadcast media if the CE does not have current contact information.
5. CEs must notify major local media outlets of a breach affecting more than 500 individuals.
6. BAs must provide notice of breach to a CE without unreasonable delay and in no event later than 60 days from discovery of the breach by the BA.

**Breaches – Duty to Mitigate Harm Remains**

The Omnibus Rule retains the need for CEs and BAs to mitigate “harm to individuals.” The Final Rule retains the statutory term “mitigate harm to individuals” to make clear that the notification should describe the steps the CE or BA is taking to mitigate potential harm to individuals resulting from the breach and that such harm is not limited to economic loss.

**VERY IMPORTANT!!!**

**Breach Notification Only Applies to “Unsecured” PHI**

Breach Notification only applies to Protected Health Information (PHI) that has not been “secured” (encrypted) according to HHS and NIST standards.

**PHI that has been secured by these standards, and is subsequently breached, *does not invoke any Breach Notification requirements*.**

The current encryption Standard referenced in the Final Rule is: “*Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*”.

(74 Federal Register, Pages 42,740-42,742)

This Breach Notification exception *does not apply* to paper, film, and other hardcopy PHI, because these materials cannot be electronically encrypted (protected) in their native forms.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 9: Privacy-Official Policy**

**Scope of Policy**

This policy governs designation of a Privacy Official for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* **PROVIDER COMPLIANCE SOLUTIONS** recognizes that the designation of a Privacy Official is mandatory under the HIPAA Rules; and that the designation of a Privacy Official provides numerous benefits to **PROVIDER COMPLIANCE SOLUTIONS.**
* **Policy Statement**
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to designate and maintain at all times an active HIPAA Privacy-Official.
* The HIPAA Privacy-Official’s general responsibilities are to:
	+ Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
	+ Conduct various risk analyses, as needed or required.
	+ Manage breach notification investigations, determinations, and responses, including breach notifications.
	+ Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.

**Procedures**

**PROVIDER COMPLIANCE SOLUTIONS**‘s HIPAA Privacy Official, and his or her designees, shall be responsible for implementing, managing, and maintaining the following procedures:

* Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
* Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
* Administer patient requests under HIPAA’s Patient Rights.
* Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
* Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
* Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
* Develop specific policies and procedures mandated by HIPAA.
* Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
* Draft and disseminate the Privacy Notice required by the Privacy Rule.
* Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
* Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
* Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
* Ensure that future initiatives are structured in such a way as to ensure patient privacy.
* Conduct periodic privacy audits and take remedial action as necessary.
* Oversee employee training in the areas of information privacy and security.
* Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
* Remain up-to-date and advise on new technologies to protect data privacy.
* Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice’s policies and procedures as necessary.
* Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
* Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
* Evaluate privacy implications of online, web-based applications.
* Monitor data collected by or posted on our website(s) for privacy concerns.
* Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations Personnel Designations - § 164.530(a)** |

1. *Standard: personnel designations*.
	1. A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
	2. A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.
2. *Implementation specification: personnel designations*. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 10: HIPAA/State Law Preemption Policy**

**Scope of Policy**

This policy governs HIPAA Preemption and State Law for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
* HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better patient and consumer access to health data than HIPAA, will generally preempt HIPAA regulations.
* HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, State Laws, or both) must be followed.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to comply, whenever possible, with both state law in the state(s) where we operate, as well as HIPAA law and regulations.

**Procedures**

* **PROVIDER COMPLIANCE SOLUTIONS**‘s designated Privacy Official shall analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
* **PROVIDER COMPLIANCE SOLUTIONS**‘s designated Privacy Official shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
* If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the **PROVIDER COMPLIANCE SOLUTIONS**‘s designated Privacy Official, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to **PROVIDER COMPLIANCE SOLUTIONS** operations.
* **PROVIDER COMPLIANCE SOLUTIONS**‘s designated Privacy Official shall conduct ongoing research to monitor legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Preemption of State Law: Definitions - Contrary - § 160.202** |

*Contrary*, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

1. A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or
2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

|  |
| --- |
| **HHS Regulations as Amended August 2002Preemption of State Law - General Rule and Exception - § 160.203** |

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

1. A determination is made by the Secretary under § 160.204 that the provision of State law:
	1. Is necessary:
		1. To prevent fraud and abuse related to the provision of or payment for health care;
		2. To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
		3. For State reporting on health care delivery or costs; or
		4. For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
	2. Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
2. The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.
3. The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
4. The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

|  |
| --- |
| **HHS Regulations Preemption of State Law: Process for Requesting Exception Determinations - § 160.204** |

1. A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:
	1. The State law for which the exception is requested;
	2. The particular standard, requirement, or implementation specification for which the exception is requested;
	3. The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
	4. How health care providers, health plans, and other entities would be affected by the exception;
	5. The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
	6. Any other information the Secretary may request in order to make the determination.
2. Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
3. The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

|  |
| --- |
| **HHS Regulations Preemption of State Law: Duration of Effectiveness of Exception Determinations - § 160.205** |

An exception granted under this subpart remains in effect until:

1. Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
2. The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

|  |
| --- |
| **HHS Regulations as Amended January 2013Preemption of State Law: Definitions - Contrary - § 160.202** |

*Contrary*, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

1. A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or
2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

|  |
| --- |
| **HHS Regulations as Amended January 2013Preemption of State Law: Definitions - More Stringent - § 160.202**  |

*More stringent* means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

1. With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
	1. Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or
	2. To the individual who is the subject of the individually identifiable health information.
2. With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.
3. With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
4. With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
5. With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

|  |
| --- |
| **HHS Regulations Preemption of State Law: Definitions - Relates to the Privacy of Individually Identifiable Health Information - § 160.202** |

*Relates to the privacy of individually identifiable health information* means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

|  |
| --- |
| **Preemption of State Law: Definitions - State Law - § 160.202** |

*State law* means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 11: HIPAA Training Policy**

**Scope of Policy**

This policy governs HIPAA Privacy and Security Training for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations concerning the training of workforce members, in accordance with the requirements at § 164.530(b).
* Clear and complete HIPAA training, in combination with appropriate HIPAA awareness resources, can significantly reduce the likelihood of breaches of confidential health information and the likelihood of HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers, and volunteers.
* HIPAA training provided by **PROVIDER COMPLIANCE SOLUTIONS** shall include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to **PROVIDER COMPLIANCE SOLUTIONS**’s operations and to the duties and responsibilities of specific individuals, workgroups, departments, and divisions.

**Procedures**

* HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA’s privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.
* HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.
* HIPAA training shall be conducted periodically for all employees, but no less than every six months.
* Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated HIPAA Privacy Official shall be responsible for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.
* The designated HIPAA Privacy Official is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.
* HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations Training - § 164.530(b)** |

1. *Standard: training*. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.
2. *Implementation specifications: training*.
	1. A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
		1. To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
		2. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
		3. To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
	2. A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

**HIPAA Commentary regarding Workforce Training...**

|  |
| --- |
| **HHS Description: Training**  |

The final regulation requires covered entities to train all members of their workforce on the policies and procedures with respect to protected health information required by this rule, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. We do not change the proposed time lines for training existing and new members of the workforce, or for training due to material changes in the covered entity’s policies and procedures. We eliminate both the requirement for employees to sign a certification following training and the triennial re-certification requirement. Covered entities are responsible for implementing policies and procedures to meet these requirements and for documenting that training has been provided.

**Policy 12: PHI Uses and Disclosures Policy**

**Scope of Policy**

This policy governs the permitted uses and disclosures of Protected Health Information for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.
* **PROVIDER COMPLIANCE SOLUTIONS** must implement policies and procedures to ensure that all uses and disclosures of PHI are made or denied in accordance with HIPAA law and regulations.
* For especially sensitive information, such as AIDS/HIV, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be *informed.* That is, made with the patient’s or consumer’s knowledge of the risks and benefits of the disclosure.
* Any disclosure of confidential patient information carries with it the potential for an unauthorized redisclosure that breaches confidentiality.
* **PROVIDER COMPLIANCE SOLUTIONS** incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under HIPAA Regulations and under State law to charge a reasonable fee to offset those costs.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to conduct its operations in full compliance with HIPAA’s Rules governing uses and disclosures of Protected Health Information.
* **PROVIDER COMPLIANCE SOLUTIONS** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.

**Procedures**

* The following priorities and time frames shall apply to requests for disclosures of PHI:
	+ *Emergency requests involving immediate emergency care of patient:* immediate processing.
	+ *Priority requests pertaining to current care of patient:*  within one workday.
	+ *Patient request for access to own record:* within three (3) workdays.
	+ *Subpoenas and depositions:* as required.
	+ *All other requests:* within five (5) workdays
* Courtesy Notifications to Practitioners – As a courtesy, records processing personnel shall notify the appropriate healthcare practitioner when any of the following occur:
	+ Patient or his or her representative requests information from the medical record.
	+ Patient or representative requests direct access to the complete medical record.
	+ Patient or representative institutes legal action.
* Disclosure Monitoring and Logging -- Medical records personnel will maintain a log to track the step-by-step process towards completion of each request for the release of PHI. Health Information Management personnel and/or the Privacy Official will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
	+ Date department received the request.
	+ Name of patient.
	+ Name and status (patient, parent, guardian) of person making request.
	+ Information released.
	+ Date released.
	+ Fee charged.
* Fee Schedule – **PROVIDER COMPLIANCE SOLUTIONS** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.
* **PROVIDER COMPLIANCE SOLUTIONS** will charge a reasonable fee to offset the costs associated with specific categories of requests. The designated HIPAA Privacy Official shall develop and implement a Fee Schedule related to disclosures of PHI. Fees shall be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and shall include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.
* Unless the request specifies release of the complete medical record, **PROVIDER COMPLIANCE SOLUTIONS** shall release only selected portions of the record. **PROVIDER COMPLIANCE SOLUTIONS** shall prepare an appropriate cover letter detailing the items included.
* Prohibition of Redisclosure -- Unless a law or regulation requires a more specific prohibition on redisclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the facility shall contain the following notice:
	+ *The attached medical information pertaining to [Name of patient] is confidential and legally privileged.* ***PROVIDER COMPLIANCE SOLUTIONS*** *has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*
* Retention of Disclosure Requests -- The designated Privacy Officer will retain the original request, the authorization for release of information, and a copy of the cover letter in the patient(s) medical record for the appropriate record retention period.
* Use of Copying Services -- To facilitate the timely processing of release of information requests, **PROVIDER COMPLIANCE SOLUTIONS** may use the services of a commercial copying service on terms that protect the integrity and confidentiality of patient information.
* Disclosure Quality Control -- The director of the Health Information Management Department and/or the designated Privacy Official shall conduct a routine audit of the release of information at least quarterly, paying particular attention to the following:
	+ Validity of authorizations.
	+ Appropriateness of information abstracted in response to the request.
	+ Retention of authorization, request, and transmitting cover letter.
	+ Procedures for telephone, electronic, and in-person requests.
	+ Compliance with designated priorities and time frames.
	+ Proper processing of fees.
	+ Maintenance of confidentiality.
* In-service Training on Disclosures -- The Director of Health Information Management and/or Privacy Official shall give periodic in-service training to all employees involved in the release of information.
* Semi-Annual Policy Review - The Director of Health Information Management and/or Privacy Official shall review this policy and associated procedures with risk management and legal counsel at least semiannually.
* Capacity to Authorize -- [Name of facility] requires a written, signed, current, valid authorization to release medical information as follows:

**Patient Category Required Signature**

**Adult Patient** The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).

**Deceased Patient** Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.

**Unemancipated Minor** Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).

**Emancipated Minor** Same as adult patients above.

**Psychiatric, drug, alcohol** Same as adult patients above, but check for

**program patients/clients** special requirements.

**AIDS/HIV or other sexually** Same as adult patients above, but check

**transmitted disease patients** for special requirements.

* Authorization Forms -- The Director of Health Information Management and/or the designated Privacy Official shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
* Revocation of Authorization -- A patient may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
* Refusal to Honor Authorization -- Health Information Management Department personnel and/or the designated Privacy Official, or others authorized to release information, will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
	+ Identity of the person presenting the authorization.
	+ Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
	+ Legal age or status as an emancipated minor.
	+ Patient capacity to understand the meaning of the authorization.
	+ Authenticity of the patient(s) signature.
	+ Current validity of the authorization.
	+ In such situations, the employee shall refer the matter to the Director of Health Information Management and/or Privacy Officer for review and decision.
* Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Person and Identity Verification Table**

| **Person to Identify** | **In-Person** **Encounter** | **Telephone****Encounter** | **Request in****Writing** (Fax, mail, hand-delivered) |
| --- | --- | --- | --- |
| **Attorney**  | 1. Presents with business card and photo identification (i.e. drivers license or organization ID badge) and:
 | 1. It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required
 | 1. Supplies business card, photo identification (i.e. driver’s license or org ID badge), letterhead. Confirmation call is required.
 |
| **Facility Directory**:  | 1. Verify identity
 | 1. Verify identity
 | 1. Verify identity
 |
| **Patient**  | 1. Patient provides name, address, and date of birth and/or social security number; or
2. Acquainted with patient
 | 1. Patient provides name, address, and date of birth and/or social security number; or
2. Acquainted with patient
 | 1. Patient provides name, address, and date of birth and/or social security number. Verify patient’s signature with that on file or on driver’s license.
 |
| **Personal Representative****(Legal Guardian) for the Patient** | 1. Personal Rep provides patient’s name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or,
2. Acquainted with personal Rep as such.
 | 1. Personal Rep provides patient’s name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or,
2. Acquainted with Personal Rep as such.
 | 1. Personal Rep provides patient’s name, address, and date of birth and/or social security number. Verify the Personal Rep’s signature with signature on file or on driver’s license.
 |
| **Persons Involved in the Patient’s Immediate Care** *(PHI relevant only to the patient’s current care (164.510(b)).*1. Blood Relative
2. Spouse
3. Domestic Partner
4. Roommate
5. Boy/Girl Friend
6. Neighbor
7. Colleague
 | 1. Patient actively involves this person in his/her care; or
2. In your best professional judgment, the disclosure is in the patient’s best interest.
 | 1. Patient actively involves this person in his/her care; or
2. In your best professional judgment, the disclosure is in the patient’s best interest.
3. Use call-back.
 | 1. N/A
 |
| **Power of Attorney For the Patient** | 1. Presents with a photo ID and a copy of the POA. Verify patient’s signature with one on file.
2. Acquainted with power of attorney as being such
 | 1. Previously obtained a copy of the POA and verified the patient’s signature with one on file.
2. Acquainted with power of attorney as being such
 | 1. Obtain a copy of the POA and verify the patient’s signature with one on file
 |
| **Provider From Another Facility** | 1. Acquainted with provider as a treatment provider;
2. Provider is wearing a photo badge from his/her facility; or,
3. Patient/personal representative introduces provider to you.
 | 1. Acquainted with provider as a treatment provider; or;
2. Call requestor back through main switchboard number (not via a direct number).
 | 1. Recognize name of facility and address on letterhead as a treatment facility; or
2. Call requestor back through main switchboard number (not via a direct number).
 |
| **Public Official** 1. CIA
2. Court Order
3. FBI
4. Law Enforcement Officer
5. OCR
6. OIG
7. Public Health Agency Official
8. Other
 | 1. Presents an agency I.D. badge;
2. Presents with a written statement of legal authority;
3. Presents with a written statement of appointment on approp. govt. letterhead;
4. Presents with warrant, court order, or legal process issued by a grand jury, or a judicial or admin. tribunal;
5. Presents with a contract for services or purchase order; or,
6. Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.
 | 1. Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.
 | 1. Written statement of legal authority;
2. Written statement of appointment on appropriate government;
3. Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or
4. Contract for services or purchase order
 |
| **Vendor Who Helps Assists w Treatment, Payment, or Health Care Operations** Examples Include, But Are Not Limited to the Following:1. Accreditation Org.
2. DME Company
3. Insurance Co.
4. Pharmacy Vendor We Have Rebate Agreement with
5. Software Vendor
6. Statement Vendor
 | 1. Recognize requestor/ organization; or
2. Photo identification with organization
 | 1. Recognize requestor or organization
 | 1. Recognize requestor/ organization; or
2. Call requestor back through main switchboard number (not via a direct number).
 |
| 1. **Workforce Member of Our Organization**
 | 1. Acquainted with individual as a workforce member; or,
2. Workforce member is wearing an I.D. badge.
 | 1. Acquainted with individual as a workforce member; or,
2. Workforce member is calling from an in-house extension.
 | 1. Request is sent from/through our own computer system; or
2. Request is on our own letterhead.
 |

**PHI Disclosures Table**

| **Requestor** | **Authorization Required?** | **Copy Fee Charged?** | **Track on Disclosure Accounting?** |
| --- | --- | --- | --- |
| **Accrediting Agencies (JCAHO, CARF)** | No | No | No |
| **Attorney for Resident** | Yes | Yes | No |
| **Attorney for Facility/Corporation** | No | No | No |
| **Contractors/ Business Associates**  | No, unless their purpose falls outside of TPO. | No | No |
| **For Deceased Persons**Coroner or Medical Examiner, Funeral DirectorsOrgan Procurement | No | No | Yes |
| **Employer*** PHI specific to work related illness or injury, and
* Required for employer’s compliance with occupational safety and health laws
 | No, for the purpose listed. Yes for all others. | No | No |
| **Family Members** | No for oral disclosures to family members involved in care;Yes for others. | Yes | No |
| Entity Subject to the Food and Drug AdministrationAdverse events, product defects or biological product deviationsTrack productsEnable product recalls, repairs, or replacementsConduct post marketing surveillance | No | No | Yes |
| **Health Oversight** * Government benefits program
* Fraud and abuse compliance
* Civil rights laws
* Trauma/tumor registries
* Vital statistics
* Reporting of abuse or neglect
 | No | No | Yes |
| **Health Care Practitioners and Providers for Continuity of Treatment and Payment** | No  | No  | No  |
| **Health Care Practitioners and Providers if not Involved in Care or Treatment (i.e., consultants)** | No  | No | No |
| **Insurance Companies/Third Party Payors** * Related to Claims Processing
 | No | No |  No |
| **Judicial and Administrative Proceedings*** Court order, or warrant
* Subpoena
 | NoNo - See Subpoena Policy  | NoYes | YesYes |
| Law Enforcement Administrative requestLocating a suspect, fugitive, material witness or missing personVictims of crimeCrimes on premisesSuspicious deathsAvert a serious threat to health or safety | No | No | Yes, except for disclosures to correctional institutions. |
| **Public Health Authorities**SurveillanceInvestigationsInterventionsForeign governments collaborating with US public health authoritiesRecording births/deathsChild/elder abusePrevent serious harmCommunicable disease  | No | No | Yes |
| **Research (w/o Authorization)** | No, if IRB or Privacy Board approves research study and waives authorization. | No | Yes |
| **Resident/Resident's Personal Representative** | No | Yes | No |
| **Specialized Government Functions**Military and Veterans' activitiesProtective services for the PresidentForeign military personnelNational security and intelligence activities | No | No | Yes, except for disclosures for national security and intelligence activities. |
| **Workers' Compensation*** Comply w/existing laws (see state law)
 | No | See applicable State Law | Yes |

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013General Rules for Uses and Disclosures of Protected Health Information: Use and Disclosure for Treatment, Payment and Health Care Operations - § 164.502(a)**  |

*Standard*. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

1. *Covered entities: Permitted uses and disclosures*. A covered entity is permitted to use or disclose protected health information as follows:
	1. To the individual;
	2. For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
	3. Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
	4. Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;
	5. Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
	6. As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).
2. *Covered entities: Required disclosures*. A covered entity is required to disclose protected health information:
	1. To an individual, when requested under, and required by § 164.524 or § 164.528; and
	2. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.
3. *Business associates: Permitted uses and disclosures*. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.
4. *Business associates: Required uses and disclosures*. A business associate is required to disclose protected health information:
	1. When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.
	2. To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.
5. *Prohibited uses and disclosures*.
	1. *Use and disclosure of genetic information for underwriting purposes*:

Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

* + 1. Except as provided in paragraph (a)(5)(i)(B) of this section:
			1. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
			2. The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
			3. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
			4. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
		2. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.
	1. *Sale of protected health information*:
		1. Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.
		2. For purposes of this paragraph, sale of protected health information means:
			1. Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.
			2. Sale of protected health information does not include a disclosure of protected health information:
			3. For public health purposes pursuant to § 164.512(b) or § 164.514(e)
			4. For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;
			5. For treatment and payment purposes pursuant to § 164.506(a);
			6. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);
			7. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;
			8. To an individual, when requested under § 164.524 or § 164.528;
			9. Required by law as permitted under § 164.512(a); and
			10. For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

|  |
| --- |
| **HHS Regulations as Amended January 2013General Rules for Uses and Disclosures of Protected Health Information: Minimum Necessary - § 164.502(b)**  |

*Standard: minimum necessary*

1. *Minimum necessary applies*. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
2. *Minimum necessary does not apply*. This requirement does not apply to:
	1. Disclosures to or requests by a health care provider for treatment;
	2. Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
	3. Uses or disclosures made pursuant to an authorization under § 164.508;
	4. Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
	5. Uses or disclosures that are required by law, as described by § 164.512(a); and
	6. Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

|  |
| --- |
| **HHS Regulations Uses and Disclosures of Protected Health Information Subject to an Agreed Upon Restriction - § 164.502(c)** |

*Standard: uses and disclosures of protected health information subject to an agreed upon restriction*. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

|  |
| --- |
| **HHS Regulations Creation of De-identified Information - § 164.502(d)** |

*Standard: uses and disclosures of de-identified protected health information*.

1. *Uses and disclosures to create de-identified information*. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.
2. *Uses and disclosures of de-identified information*. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:
	1. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and
	2. If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

|  |
| --- |
| **HHS Regulations as Amended January 2013General Rules for Uses and Disclosures of Protected Health Information: Disclosures to Business Associates - § 164.502(e)**  |

1. *Standard: disclosures to business associates*.
	1. A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
	2. A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.
2. *Implementation specification: documentation*. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

|  |
| --- |
| **HHS Regulations as Amended January 2013General Rules for Uses and Disclosures of Protected Health Information: Deceased Individuals - § 164.502(f)** |

*Standard: deceased individuals*. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

|  |
| --- |
| **HHS Regulations as Amended August 2002Personal Representatives - § 164.502(g)**  |

1. *Standard: personal representatives*. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.
2. *Implementation specification: adults and emancipated minors*. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
3. *Implementation specification: unemancipated minors*.
	1. If under applicable law a parent, guardian, or other person acting in *loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:
		1. The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
		2. The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or
		3. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.
	2. Notwithstanding the provisions of paragraph (g)(3)(i) of this section:
		1. If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.
		2. If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.
		3. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraph (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.
4. *Implementation specification: deceased individuals*. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
5. *Implementation specification: abuse, neglect, endangerment situations*. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:
	1. The covered entity has a reasonable belief that:
		1. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
		2. Treating such person as the personal representative could endanger the individual; and
	2. The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

|  |
| --- |
| **HHS Regulations Confidential Communications - § 164.502(h)** |

*Standard: confidential communications*. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

|  |
| --- |
| **HHS Regulations Uses and Disclosures Consistent With Notice - § 164.502(i)** |

*Standard: uses and disclosures consistent with notice*. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

|  |
| --- |
| **HHS Regulations Disclosures by Whistleblowers and Workforce Member Crime Victims - § 164.502(j)** |

*Standard: disclosures by whistleblowers and workforce member crime victims*.

1. *Disclosures by whistleblowers*. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:
	1. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
	2. The disclosure is to:
		1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
		2. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.
2. *Disclosures by workforce members who are victims of a crime*. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
	1. The protected health information disclosed is about the suspected perpetrator of the criminal act; and
	2. The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 13: Patient Rights Policy**

**Scope of Policy**

This policy governs the provision and management of Patient Rights for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements pertaining to the rights of patients at § 164.520, to § 164.528, as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
* Patient information related to patient rights includes only that information contained in each patient’s Designated Record Set (“DRS”), which is defined in the HIPAA regulations at § 164.501 as:
	+ A group of records maintained by or for a covered entity that is:
		- The medical records and billing records about individuals maintained by or for a covered health care provider;
		- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
		- Used, in whole or in part, by or for the covered entity to make decisions about individuals.
	+ The term “record” means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
* The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable health information.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide all the patient rights to our patients that are called for in the HIPAA regulations.
* Patient Rights that we provide and support include:
* The Right to receive a copy of our “Notice of Privacy Practices”, which details how individually identifiable health information may be used or disclosed by this organization.
* The Right to review or obtain a copy of medical records about that patient, or about the patient’s minor children.
* The Right to request restrictions on the use or disclosure of the patient’s medical records.
* The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
* The Right to request amendments to medical records, with certain limitations.
* The Right to an accounting of certain disclosures of individually identifiable health information.
* The Right to file a privacy complaint directly with us, or with the federal government.
* No retaliation of any kind is permitted against any person, patient, or workforce member for exercising any Right guaranteed by HIPAA.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** that our Designated Record Set, for purposes of fulfilling HIPAA Patient Rights *includes* the following types or categories of data and items:
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** that our Designated Record Set, for purposes of fulfilling HIPAA Patient Rights *excludes* the following types or categories of data and items:
	+ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Procedures**

* Each patient is to receive a copy of this offices updated Notice of Privacy Practices.
* Post a copy in a conspicuous location in our waiting room.
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations Notice of Privacy Practices: Right to Notice - § 164.520(a)** |

*Standard: notice of privacy practices*.

1. *Right to notice*. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to protected health information.
2. *Exception for group health plans*.
	1. An individual enrolled in a group health plan has a right to notice:
		1. From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or
		2. From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.
	2. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has dis-enrolled from a health insurance issuer or HMO offered by the plan, must:
		1. Maintain a notice under this section; and
		2. Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.
	3. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has dis-enrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.
3. *Exception for inmates*. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

|  |
| --- |
| **HHS Regulations as Amended January 2013Notice of Privacy Practices: Provision of the Notice - § 164.520(c)**  |

*Implementation specifications: provision of notice*. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

1. *Specific requirements for health plans*.
	1. A health plan must provide the notice:
		1. No later than the compliance date for the health plan, to individuals then covered by the plan;
		2. Thereafter, at the time of enrollment, to individuals who are new enrollees.
	2. No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.
	3. The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.
	4. If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.
	5. If there is a material change to the notice:
		1. A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.
		2. A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.
2. *Specific requirements for certain covered health care providers*. A covered health care provider that has a direct treatment relationship with an individual must:
	1. Provide the notice:
		1. No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or
		2. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.
	2. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reasons why the acknowledgment was not obtained.
	3. If the covered health care provider maintains a physical service delivery site:
		1. Have the notice available at the service delivery site for individuals to request to take with them; and
		2. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and
	4. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.
3. *Specific requirements for electronic notice*.
	1. A covered entity that maintains a web site that provides information about the covered entity’s customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.
	2. A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.
	3. For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.
	4. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

|  |
| --- |
| **HHS Regulations as Amended January 2013Right of Individual to Request Restriction of Uses and Disclosures of PHI - § 164.522(a)** |

1. *Standard: right of an individual to request restriction of uses and disclosures*.
	1. A covered entity must permit an individual to request that the covered entity restrict:
		1. Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and
		2. Disclosures permitted under § 164.510(b).
	2. Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.
	3. A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.
	4. If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.
	5. A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.
	6. A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:
		1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
		2. The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.
2. *Implementation specifications: terminating a restriction*. A covered entity may terminate its agreement to a restriction, if:
	1. The individual agrees to or requests the termination in writing;
	2. The individual orally agrees to the termination and the oral agreement is documented; or
	3. The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:
		1. Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and
		2. Only effective with respect to protected health information created or received after it has so informed the individual.
3. *Implementation specification: documentation*. A covered entity must document a restriction in accordance with Sec. 160.530(j) of this subchapter.

|  |
| --- |
| **HHS Regulations Rights to Request Privacy Protection: Confidential Communications - § 164.522(b)** |

1. *Standard: confidential communications requirements*.
	1. A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
	2. A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,
2. *Implementation specifications: conditions on providing confidential communications*.
	1. A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.
	2. A covered entity may condition the provision of a reasonable accommodation on:
		1. When appropriate, information as to how payment, if any, will be handled; and
		2. Specification of an alternative address or other method of contact.
	3. A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
	4. A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

|  |
| --- |
| **HHS Regulations Access to Protected Health Information - § 164.524(a)** |

*Standard: access to protected health information*.

1. *Right of access*. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:
	1. Psychotherapy notes;
	2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
	3. Protected health information maintained by a covered entity that is:
		1. Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
		2. Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
2. *Unreviewable grounds for denial*. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.
	1. The protected health information is excepted from the right of access by paragraph (a)(1) of this section.
	2. A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate’s request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
	3. An individual’s access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
	4. An individual’s access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
	5. An individual’s access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
3. *Reviewable grounds for denial*. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:
	1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
	2. The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
	3. The request for access is made by the individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
4. *Review of a denial of access*. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

|  |
| --- |
| **HHS Regulations as Amended January 2013Access of Individuals to Protected Health Information: Requests for Access and Timely Action - § 164.524(b)** |

*Implementation specifications: requests for access and timely action*.

1. *Individual’s request for access*. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.
2. *Timely action by the covered entity*.
	1. Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.
		1. If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.
		2. If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.
	2. If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:
		1. The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
		2. The covered entity may have only one such extension of time for action on a request for access.

|  |
| --- |
| **HHS Regulations as Amended January 2013Access of Individuals to Protected Health Information: Provision of Access - § 164.524(c)** |

*Implementation specifications: provision of access*. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. *Providing the access requested*. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.
2. *Form of access requested*.
	1. The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.
	2. Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.
	3. The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:
		1. The individual agrees in advance to such a summary or explanation; and
		2. The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
3. *Time and manner of access*.
	1. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual’s request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
	2. If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.
4. *Fees*. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
	1. Labor for copying the protected health information requested by the individual, whether in paper or electronic form;
	2. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
	3. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
	4. Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

|  |
| --- |
| **HHS Regulations Access of Individuals to Protected Health Information: Denial of Access - § 164.524(d)** |

*Implementation specifications: denial of access*. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

1. *Making other information accessible*. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.
2. *Denial*. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:
	1. The basis for the denial;
	2. If applicable, a statement of the individual’s review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and
	3. A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).
3. *Other responsibility*. If the covered entity does not maintain the protected health information that is the subject of the individual’s request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.
4. *Review of denial requested*. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official’s determination.

|  |
| --- |
| **HHS Regulations Right to Amend - § 164.526(a)** |

*Standard: right to amend*.

1. *Right to amend*. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.
2. *Denial of amendment*. A covered entity may deny an individual’s request for amendment, if it determines that the protected health information or record that is the subject of the request:
	1. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
	2. Is not part of the designated record set;
	3. Would not be available for inspection under § 164.524; or
	4. Is accurate and complete.

|  |
| --- |
| HHS Regulations as Amended August 2002Right to an Accounting of Disclosures - § 164.528(a)  |

*Standard: right to an accounting of disclosures of protected health information*.

1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:
	1. To carry out treatment, payment and health care operations as provided in § 164.506;
	2. To individuals of protected health information about them as provided in § 164.502;
	3. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
	4. Pursuant to an authorization as provided in § 164.508;
	5. For the facility’s directory or to persons involved in the individual’s care or other notification purposes as provided in § 164.510;
	6. For national security or intelligence purposes as provided in § 164.512(k)(2);
	7. To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
	8. As part of a limited data set in accordance with § 164.514(e); or
	9. That occurred prior to the compliance date for the covered entity.
	10. The covered entity must temporarily suspend an individual’s right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
	11. If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:
		1. Document the statement, including the identity of the agency or official making the statement;
		2. Temporarily suspend the individual’s right to an accounting of disclosures subject to the statement; and
		3. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.
2. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

|  |
| --- |
| **HHS RegulationsThe Administrative Requirements: Waiver of Rights - § 164.530(h)** |

*Standard: waiver of rights*. A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 14: Privacy Complaints Policy**

**Scope of Policy**

This policy governs the privacy complaints process for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
* HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.
* Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Privacy Officer, who shall establish a process and appropriate forms to receive and process complaints.

**Procedures**

* All complaints must be submitted in written form, dated and signed by the complainant.
* **PROVIDER COMPLIANCE SOLUTIONS** shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.
* The designated HIPAA Officer shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
* The final resolution or disposition of each complaint shall be documented in accordance with **PROVIDER COMPLIANCE SOLUTIONS**‘s Documentation Policy, and shall be retained in accordance with **PROVIDER COMPLIANCE SOLUTIONS**‘s Documentation Retention Policy.
* The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
* In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediations may include, but are not limited to:
	+ A written apology to the complainant from our organization.
	+ Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
	+ Financial compensation, if determined to be appropriate by legal counsel and senior management.
	+ Sanctions against workforce members, as appropriate to the circumstances.
	+ Other unspecified remediation(s), as determined by legal counsel and senior management.
* For complaints submitted to the federal government, it is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in **PROVIDER COMPLIANCE SOLUTIONS**’s HHS Investigations Policy.
* No officer, agent, employee, contractor, temporary worker, or volunteer of **PROVIDER COMPLIANCE SOLUTIONS** shall obstruct or impede any investigation in any way, whether internal or federal.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations The Administrative Requirements: Complaints to the Covered Entity - § 164.530(d)** |

1. *Standard: complaints to the covered entity*. A covered entity must provide a process for individuals to make complaints concerning the covered entity’s policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.
2. *Implementation specification: documentation of complaints*. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 15: Risk Management Process Policy**

**Scope of Policy**

This policy governs the establishment and maintenance of a Risk Management Process for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

**Policy Statement**

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this policy.

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish, implement, and maintain an appropriate risk management process.
* Such a risk management process shall be under the direct control and supervision of the designated Privacy Official, and shall involve legal counsel, information technology, records management, senior management, and any other parties or persons deemed to be appropriate to the process.
* Business and information-technology “best practices”, along with the research and recommendations of the National Institute for Standards and Technology (“NIST”), shall be included in the development and execution of the risk management process.
* Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
* The results of the risk management process shall be input into management’s decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.
* **Procedures**
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**OCR Guidance on HIPAA Risk Analysis (07-14-2010)**

**Introduction**

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

**We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A).**

Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. **Risk analysis is the first step in that process.**

We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.

**Risk Analysis Requirements under the Security Rule**

The Security Management Process standard in the Security Rule requires organizations to *“Implement policies and procedures to prevent, detect, contain, and correct security violations.”* (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard.

Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required).

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

The following questions adapted from NIST Special Publication (SP) 800-665 are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing the Security Rule:

* Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
* What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
* What are the human, natural, and environmental threats to information systems that contain e-PHI?

In addition to an express requirement to conduct a risk analysis, the Rule indicates that risk analysis is a necessary tool in reaching substantial compliance with many other standards and implementation specifications.

For example, the Rule contains several implementation specifications that are labeled “addressable” rather than “required.” (68 FR 8334, 8336 (Feb. 20, 2003).) An addressable implementation specification is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so.

(See 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306(d)(3).)

The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Organizations should use the information gleaned from their risk analysis as they, for example:

* Design appropriate personnel screening processes. (45 C.F.R. § 164.308(a)(3)(ii)(B).)
* Identify what data to backup and how. (45 C.F.R. § 164.308(a)(7)(ii)(A).)
* Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a)(2)(iv) and (e)(2)(ii).)
* Address what data must be authenticated in particular situations to protect data integrity. (45 C.F.R. § 164.312(c)(2).)
* Determine the appropriate manner of protecting health information transmissions. (45 C.F.R. § 164.312(e)(1).)

**Important Definitions**

Unlike “availability”, “confidentiality” and “integrity”, the following terms are not expressly defined in the Security Rule. The definitions provided in this guidance, which are consistent with common industry definitions, are provided to put the risk analysis discussion in context. These terms do not modify or update the Security Rule and should not be interpreted inconsistently with the terms used in the Security Rule.

**Vulnerability**

Vulnerability is defined in NIST Special Publication (SP) 800-30 as *“[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”* Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of e-PHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical.

* Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines.
* Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

**Threat**

An adapted definition of threat, from NIST SP 800-30, is “*The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

* Natural threats such as floods, earthquakes, tornadoes, and landslides.
* Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
* Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

**Risk**

An adapted definition of risk, from NIST SP 800-30, is:*“The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . Risks arise from legal liability or mission loss due to:*

1. *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
2. *Unintentional errors and omissions*
3. *IT disruptions due to natural or man- made disasters*
4. *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk can be understood as a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

**Elements of a Risk Analysis**

There are numerous methods of performing risk analysis and there is no single method or “best practice” that guarantees compliance with the Security Rule. Some examples of steps that might be applied in a risk analysis process are outlined in NIST SP 800-30.6

The remainder of this guidance document explains several elements a risk analysis must incorporate, regardless of the method employed.

**Scope of the Analysis**

*The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)*

This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization’s risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

**Data Collection**

An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

**Identify and Document Potential Threats and Vulnerabilities**

Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities that, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

**Assess Current Security Measures**

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

The security measures implemented to reduce risk will vary among organizations. For example, small organizations tend to have more control within their environment. Small organizations tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e- PHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a small organization may differ

from those that are appropriate in large organizations.

**Determine the Likelihood of Threat Occurrence**

The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are “reasonably anticipated.”

The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**Determine the Potential Impact of Threat Occurrence**

The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**Determine the Level of Risk**

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

Finalize Documentation

The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).) The risk analysis documentation is a direct input to the risk management process.

**Periodic Review and Updates to the Risk Assessment**

The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. For example, if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate

levels.

**In Summary**

Risk analysis is the first step in an organization’s Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.

**Resources**

The Security Series papers available on the Office for Civil Rights (OCR) website, http://www.hhs.gov/ocr/hipaa, contain a more detailed discussion of tools and methods available for risk analysis and risk management, as well as other Security Rule compliance requirements.

Visit http://www.hhs.gov/ocr/hipaa for the latest guidance,

FAQs and other information on the Security Rule.

Several other federal and non-federal organizations have developed materials that might be helpful to covered entities seeking to develop and implement risk analysis and risk management strategies. The Department of Health and Human Services does not endorse or recommend any particular risk analysis or risk management model. The documents referenced below do not constitute legally binding guidance for covered entities, nor does adherence to any or all of the standards contained in these materials prove substantial compliance with the risk analysis requirements of the Security Rule. Rather, the materials

are presented as examples of frameworks and methodologies that some organizations use to guide their risk analysis efforts.

The National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, is responsible for developing information security standards for federal agencies. NIST has produced a series of Special Publications, available at http://csrc.nist.gov/publications/PubsSPs.html, which provide information that is relevant to information technology security. These papers include:

* *Guide to Technical Aspects of Performing Information Security Assessments* (SP800- 115).
* *Information Security Handbook: A Guide for Managers* (SP800-100; Chapter 10 provides a Risk Management Framework and details steps in the risk management process).
* *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (SP800-66; Part 3 links the NIST Risk Management Framework to components of the Security Rule).
* A draft publication, *Managing Risk from Information Systems* (SP800-39).

The Office of the National Coordinator for Health Information Technology (ONC) has produced a risk assessment guide for small health care practices, called Reassessing Your Security Practices in a Health IT Environment, which is available at:

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS\_0\_10741\_848086\_0\_0\_18/SmallPracticeSecurityGuide-1.pdf.

The Healthcare Information and Management Systems Society (HIMSS), a private consortium of health care information technology stakeholders, created an information technology security practices questionnaire, available at:

<http://www.himss.org/content/files/ApplicationSecurityv2.3.pdf>.

The questionnaire was developed to collect information about the state of IT security in the health care sector, but could also be a helpful self-assessment tool during the risk analysis process.

The Health Information Trust Alliance (HITRUST) worked with industry to create the Common Security Framework (CSF), a proprietary resource available at:

<http://hitrustcentral.net/files>.

The risk management section of the document, *Control Name: 03.0*, explains the role of risk assessment and management in overall security program development and implementation. The paper describes methods for implementing a risk analysis program, including knowledge and process requirements, and it links various existing frameworks and standards to applicable points in an information security life cycle.

**HIPAA Regulations – General Rules for compliance with the Security Rule.**

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: General Rules - § 164.306** |

1. *General requirements*. Covered entities and business associates must do the following:
	1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
	2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
	3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
	4. Ensure compliance with this subpart by its workforce.
2. *Flexibility of approach*.
	1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
	2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
		1. The size, complexity, and capabilities of the covered entity or business associate.
		2. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
		3. The costs of security measures.
		4. The probability and criticality of potential risks to electronic protected health information.
3. *Standards*. A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.
4. *Implementation specifications*. In this subpart:
	1. Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.
	2. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.
	3. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must--
		1. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
		2. As applicable to the covered entity or business associate--
			1. Implement the implementation specification if reasonable and appropriate; or
			2. If implementing the implementation specification is not reasonable and appropriate--
				1. Document why it would not be reasonable and appropriate to implement the implementation specification; and
				2. Implement an equivalent alternative measure if reasonable and appropriate.
5. *Maintenance*. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Policy 16: Risk Analysis Policy**

**Scope of Policy**

This policy governs Risk Analysis for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the requirements at § 164.308(a)(1).
* Risk analysis is an integral part of this organization’s overall Risk Management Process Policy and process.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (“ePHI”) that we are entrusted with.
* Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Official or HIPAA Privacy Officer, who shall establish a plan and procedures for the conduct of such analyses.

**Procedures**

* All such risk analyses and assessments shall be conducted periodically, but at least Specify Time Interval (at least annually is suggested).
* The risk analysis process shall be modeled upon the risk analysis process recommended by the National Institute for Standards and Technology (“NIST”).
* The results of risk analyses and assessments shall become an integral part of management’s decision-making process, and shall guide decisions related to the protection of Protected Health Information
* All such risk analyses and assessments shall be documented in accordance with this organization’s Documentation Policy and HIPAA Regulations.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**Security Rule Requirements for Risk Analysis and Risk Management**

The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to *“[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.”*

The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are **Risk Analysis** and **Risk Management**.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”*

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to *“[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)].”*

Both risk analysis and risk management are standard information security processes and are critical to a covered entity’s Security Rule compliance efforts. As stated in the responses to public comment in the Preamble to the Security Rule, risk analysis and risk management are important to covered entities since these processes will *“form the foundation upon which an entity’s necessary security activities are built.” (68 Fed. Reg. 8346.)*

Much of the content included in this paper is adapted from government resources such as the

National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP),

specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. These

government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, “*Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization’s implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.*”

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

**Important Definitions to Understand**

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including “vulnerability,” “threat,” and “risk,” and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

**VULNERABILITY**

Vulnerability is defined in NIST SP 800-30 as *“[a] flaw or weakness in system security*

*procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”*

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

**THREAT**

An adapted definition of threat, from NIST SP 800-30, is “*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and nvironmental. Examples of common threats in each of these general categories include:

* Natural threats may include floods, earthquakes, tornadoes, and landslides.
* Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
* Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

**RISK**

The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

”*The net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur.*

*…[R]isks arise from legal liability or mission loss due to—*

1. *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
2. *Unintentional errors and omissions*
3. *IT disruptions due to natural or man-made disasters*
4. *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

**Example Risk Analysis and Risk Management Steps**

There are numerous methods of performing risk analysis and risk management. There is no single method or “best practice” that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

**EXAMPLE RISK ANALYSIS STEPS:**

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat/occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.

**EXAMPLE RISK MANAGEMENT STEPS:**

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity “must document” a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

**Example Risk Analysis Steps**

As previously stated, the Security Rule requires covered entities to conduct an accurate and

thorough risk analysis. This section of the paper provides an example approach to risk analysis

which may be used by covered entities.

**1. Identify the Scope of the Analysis**

Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

*“(1) Electronic storage media including memory devices in computers*

*(hard drives) and any removable/transportable digital memory medium,*

*such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission*

*media used to exchange information already in electronic storage media. Transmission*

*media include, for example, the internet (wide-open), extranet (using internet*

*technology to link a business with information accessible only to collaborating parties),*

*leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of*

*voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.”*

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity’s risk analysis should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

**2. Gather Data**

Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.

The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity’s environment and amount of EPHI held. For example, a small provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple

physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

**3. Identify and Document Potential Threats and Vulnerabilities**

Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps, but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

**IDENTIFY AND DOCUMENT THREATS**

Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats.

Covered entities may identify different threats unique to the circumstances of their environment. After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

**IDENTIFY AND DOCUMENT VULNERABILITIES**

While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of

information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered

entities. In contrast, small covered entities will likely rely on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

**4. Assess Current Security Measures**

The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and nontechnical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability

and responsibility, and physical and environmental security measures.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EHPI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**5. Determine the Likelihood of Threat Occurrence**

Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

“Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used to express the likelihood of occurrence. The ratings used will depend on the covered entity’s approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

* High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).
* Medium Likelihood – a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
* Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

* Unauthorized access to or disclosure of EPHI.
* Permanent loss or corruption of EPHI.
* Temporary loss or unavailability of EPHI.
* Loss of financial cash flow.
* Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

**QUALITATIVE METHOD**

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

**QUANTITATIVE METHOD**

In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**7. Determine the Level of Risk**

Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity’s risk level determination to reasonably anticipated risks to EPHI.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of “high” combined with an impact value of “low” may equal a risk level of “low.” Or a threat likelihood value of “medium” combined with an impact value of “medium” may equal a risk level of “medium.”

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of “high” could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional

information to prioritize risk management efforts. One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2),

164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**8. Identify Security Measures and Finalize Documentation**

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization’s policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation. This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section “Example Risk Management Steps.”

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

**Example Risk Management Steps**

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

**1. Develop and Implement a Risk Management Plan**

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity’s evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity’s workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

* Should certain risks be addressed immediately or in the future?
* Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

* Risks (threat and vulnerability combinations) being addressed;
* Security measures selected to reduce the risks;
* Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity’s actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

**2. Implement Security Measures**

Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget.

Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

**3. Evaluate and Maintain Security Measures**

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk

analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

*“Security measures implemented to comply with standards and*

*implementation specifications adopted under § 164.105 [(the*

*Organizational Requirements)] and this subpart [(the Security Rule)] must*

*be reviewed and modified as needed to continue provision of reasonable*

*and appropriate protection of [EPHI] as described at § 164.316.”*

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

“*Perform a periodic technical and nontechnical evaluation, based initially*

*upon the standards implemented under this rule and subsequently, in*

*response to environmental or operational changes affecting the security of*

*[EPHI], that establishes the extent to which an entity’s security polices*

*and procedures meet the requirements of [the Security Rule].”*

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the EPHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

**In Summary**

Risk analysis and risk management are the foundation of a covered entity’s Security Rule compliance efforts. Risk analysis and risk management are on going processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

**Policy 17: Risk Management Implementation Policy**

**Scope of Policy**

This policy governs Risk Management Implementation for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to risk management implementation, in accordance with the requirements at § 164.308(a)(1).
* Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
* This Risk Management Implementation Policy shall be considered an integral part of our other Risk Management policies, including, but not limited to, our:
	+ Risk Management Process Policy, and our
	+ Risk Analysis Policy

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully and completely implement our risk management process and all related policies.
* The implementation of our risk management process, analyses, and improvements shall be under the direct supervision of the designated HIPAA Official or HIPAA Officer.
* The designated HIPAA Official or HIPAA Officer shall develop and implement a plan, procedures, and a timetable for the implementation of our risk management process in all its aspects. Such actions shall be consistent with our other risk management policies.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**Security Rule Requirements for Risk Analysis and Risk Management**

The Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to *“[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.”*

The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are **Risk Analysis** and **Risk Management**.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”*

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to *“[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)].”*

Both risk analysis and risk management are standard information security processes and are critical to a covered entity’s Security Rule compliance efforts. As stated in the responses to public comment in the Preamble to the Security Rule, risk analysis and risk management are important to covered entities since these processes will *“form the foundation upon which an entity’s necessary security activities are built.” (68 Fed. Reg. 8346.)*

Much of the content included in this paper is adapted from government resources such as the

National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP),

specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. These

government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, “*Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization’s implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.*”

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

**Important Definitions to Understand**

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including “vulnerability,” “threat,” and “risk,” and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

**VULNERABILITY**

Vulnerability is defined in NIST SP 800-30 as *“[a] flaw or weakness in system security*

*procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”*

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

**THREAT**

An adapted definition of threat, from NIST SP 800-30, is “*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and nvironmental. Examples of common threats in each of these general categories include:

* Natural threats may include floods, earthquakes, tornadoes, and landslides.
* Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
* Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

**RISK**

The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

”*The net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur.*

*…[R]isks arise from legal liability or mission loss due to—*

1. *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
2. *Unintentional errors and omissions*
3. *IT disruptions due to natural or man-made disasters*
4. *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

**Example Risk Analysis and Risk Management Steps**

There are numerous methods of performing risk analysis and risk management. There is no single method or “best practice” that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

**EXAMPLE RISK ANALYSIS STEPS:**

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat/occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.

**EXAMPLE RISK MANAGEMENT STEPS:**

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity “must document” a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

**Example Risk Analysis Steps**

As previously stated, the Security Rule requires covered entities to conduct an accurate and thorough risk analysis. This section of the paper provides an example approach to risk analysis which may be used by covered entities.

**1. Identify the Scope of the Analysis**

Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

*“(1) Electronic storage media including memory devices in computers*

*(hard drives) and any removable/transportable digital memory medium,*

*such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission*

*media used to exchange information already in electronic storage media. Transmission*

*media include, for example, the internet (wide-open), extranet (using internet*

*technology to link a business with information accessible only to collaborating parties),*

*leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of*

*voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.”*

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity’s risk analysis should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

**2. Gather Data**

Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.

The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity’s environment and amount of EPHI held. For example, a small provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

**3. Identify and Document Potential Threats and Vulnerabilities**

Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps, but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

**IDENTIFY AND DOCUMENT THREATS**

Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats.

Covered entities may identify different threats unique to the circumstances of their environment. After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

**IDENTIFY AND DOCUMENT VULNERABILITIES**

While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of

information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered

entities. In contrast, small covered entities will likely rely on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

**4. Assess Current Security Measures**

The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and nontechnical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability

and responsibility, and physical and environmental security measures.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EHPI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**5. Determine the Likelihood of Threat Occurrence**

Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

“Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used to express the likelihood of occurrence. The ratings used will depend on the covered entity’s approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

* High Likelihood – a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).
* Medium Likelihood – a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
* Low Likelihood – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

* Unauthorized access to or disclosure of EPHI.
* Permanent loss or corruption of EPHI.
* Temporary loss or unavailability of EPHI.
* Loss of financial cash flow.
* Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

**QUALITATIVE METHOD**

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

**QUANTITATIVE METHOD**

In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**7. Determine the Level of Risk**

Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity’s risk level determination to reasonably anticipated risks to EPHI.

The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

A risk level matrix can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of “high” combined with an impact value of “low” may equal a risk level of “low.” Or a threat likelihood value of “medium” combined with an impact value of “medium” may equal a risk level of “medium.”

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of “high” could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional

information to prioritize risk management efforts. One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2),

164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

**8. Identify Security Measures and Finalize Documentation**

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization’s policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation. This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section “Example Risk Management Steps.”

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

**Example Risk Management Steps**

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

**1. Develop and Implement a Risk Management Plan**

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity’s evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity’s workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

* Should certain risks be addressed immediately or in the future?
* Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

* Risks (threat and vulnerability combinations) being addressed;
* Security measures selected to reduce the risks;
* Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity’s actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

**2. Implement Security Measures**

Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget.

Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

**3. Evaluate and Maintain Security Measures**

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk

analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

*“Security measures implemented to comply with standards and*

*implementation specifications adopted under § 164.105 [(the*

*Organizational Requirements)] and this subpart [(the Security Rule)] must*

*be reviewed and modified as needed to continue provision of reasonable*

*and appropriate protection of [EPHI] as described at § 164.316.”*

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

“*Perform a periodic technical and nontechnical evaluation, based initially*

*upon the standards implemented under this rule and subsequently, in*

*response to environmental or operational changes affecting the security of*

*[EPHI], that establishes the extent to which an entity’s security polices*

*and procedures meet the requirements of [the Security Rule].”*

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the EPHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

**In Summary**

Risk analysis and risk management are the foundation of a covered entity’s Security Rule compliance efforts. Risk analysis and risk management are on going processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 18: Sanction Policy**

**Scope of Policy**

This policy governs Workforce Sanctions and disciplinary actions for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).
* Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions; can help prevent breaches of individually identifiable health information and Protected Health Information, and can help prevent, or reduce the severity, of HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established policies and procedures, or who commit various offenses.
* Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
* Certain offenses can invoke immediate termination, including, but not limited to:
	+ Theft
	+ Intentional lying or deception
	+ Drug or alcohol use while on the job
	+ Violence against persons or property
* Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all workforce sanctions and their dispositions, according to our Documentation Policy and HIPAA requirements.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations The Administrative Requirements: Sanctions - § 164.530(e)** |

1. *Standard: sanctions*. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.
2. *Implementation specification: documentation*. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

|  |
| --- |
| **HHS Description The Administrative Requirements: Sanctions** |

In § 164.518(e) of the NPRM, we proposed to require all covered entities to develop, and apply when appropriate, sanctions against members of its workforce who failed to comply with privacy policies or procedures of the covered entity or with the requirements of the rule. Covered entities would be required to develop and impose sanctions appropriate to the nature of the violation. The preamble stated that the type of sanction applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination. The NPRM preamble language also stated that covered entities would be required to apply sanctions against business associates that violated the proposed rule.

In the final rule, we retain the requirement for sanctions against members of a covered entity's workforce. We also require a covered entity to have written policies and procedures for the application of appropriate sanctions for violations of this subpart and to document those sanctions. These sanctions do not apply to whistleblower activities that meet the provisions of § 164.502(j) or complaints, investigations, or opposition that meet the provisions of § 164.530(g)(2). We eliminate language regarding business associates from this section. Requirements with respect to business associates are stated in § 164.504.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 19: Information Systems Activity Review Policy**

**Scope of Policy**

This policy governs Information Systems Activity Reviews for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to information systems activity review, in accordance with the requirements at § 164.308(a)(1).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
* The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all information system activity review activities and efforts.
* This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. ***Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 20: Assignment of Security Responsibility Policy**

**Scope of Policy**

This policy governs the Assignment of Responsibility for health information data security for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
* The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
* The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the (Insert Name) designated HIPAA Official or Officer, who shall report directly to Name of Direct Report .

**Procedures**

The (Insert Name) designated HIPAA Official or Officer shall implement the following procedures, as appropriate, in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Risk Management policies:

* Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
* Maintain an accurate inventory of (1) all individuals who have access to the Practice’s confidential information, including PHI, and (2) all uses and disclosures of the Practice’s confidential information by any person or entity.
* Administer patient requests and processes under HIPAA’s patient rights.
* Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
* Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
* Work with appropriate technical personnel to protect the Practice’s confidential information from unauthorized use or disclosure.
* Develop specific policies and procedures mandated by the Privacy Rule.
* Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
* Draft and disseminate the privacy notice required by the Privacy Rule.
* Determine when the Practice might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
* Ensure that any research efforts conducted or supported by the Practice comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
* Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that the Practice’s confidential data is adequately protected when such access is granted.
* Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
* Ensure that future Practice initiatives are structured in such a way to ensure patient privacy.
* Conduct periodic privacy audits and take remedial action as necessary.
* Oversee employee training in the area of privacy.
* Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
* Remain up-to-date and advise on new technologies to protect data privacy.
* Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice’s policies and procedures as necessary.
* Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
* Anticipate members’ concerns and questions about the Practice’s use of their confidential information and develop policies and procedures to respond to those concerns and questions.
* Evaluate privacy implications of any future on-line, web-based application procedure.
* Monitor any data collected by or posted on the Practice’s Web sites for privacy concerns.
* Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the Practice’s privacy practices.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. ***Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.**

**HHS Commentaries regarding the Assignment of Security Responsibility...**

*Assigned Security Responsibility (§ 164.308(a)(2))*

We proposed that the responsibility for security be assigned to a specific individual or organization to provide an organizational focus and importance to security, and that the assignment be documented. Responsibilities would include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.

In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 21: Authorization and Supervision Policy**

**Scope of Policy**

This policy governs the authorization and supervision of health data-related access and activities for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).
* Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
* Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, are essential components of a well-managed risk management system.
* Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, can help reduce our overall risk, and reduce the likelihood of data breaches and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to only permit workforce members who have been appropriately authorized, to have access to individually identifiable health information.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to properly and appropriately supervise workforce members who have access to individually identifiable health information.
* Workforce members of **PROVIDER COMPLIANCE SOLUTIONS** shall have access only to the individually identifiable health information that they need in order to perform their work-related duties.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document the authorization and supervision of all workforce members who have access to individually identifiable health information.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. ***Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.**

**NIST Guidance regarding Authorization and Supervision Procedures**

**Key Activities related to Authorization and Supervision Procedures...**

* Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
* Decide how access will be granted to workforce members within the organization.
* Select the basis for restricting access.
* Select an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access.)
* Determine if direct access to EPHI will ever be appropriate for individuals external to the organization (e.g., business partners or patients seeking access to their own EPHI).

**Questions to Consider...**

* Do the organization’s IT systems have the capacity to set access controls?
* Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?
* Does the organization grant remote access to EPHI?
* What method(s) of access control is (are) used (e.g., identity-based, role-based, location-based, or a combination)?
* Are duties separated such that only the minimum necessary EPHI is made available to each staff member based on their job requirements?

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 22: Workforce Clearance Policy**

**Scope of Policy**

This policy governs Workforce Clearance and Screening (pre-employment and post-employment) for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce clearance, in accordance with the requirements at § 164.308(a)(3).
* Providing for appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
* The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member’s job and its associated duties and responsibilities. Workforce members shall have access to all of the individually identifiable health information that they need to do their jobs, but no more access than that.
* No member of the workforce shall have access to a higher level of individually identifiable health information than the level for which they have been cleared.
* The designated HIPAA Official or HIPAA Officer shall develop specific procedures to ensure that the intent of this policy is executed in fact.
* Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to individually identifiable health information.
* The designated HIPAA Official or HIPAA Officer shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all workforce clearance-related activities and efforts.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Regulations regarding Workforce Clearance...**

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. ***Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.**

**HHS Responses to Comments regarding Workforce Security & Workforce Clearance...**

**Workforce Security (§ 164.308(a)(3))**

*Comment*: The majority of comments concerned the supervision of maintenance personnel by an authorized knowledgeable person. Commenters stated this would not be feasible in smaller settings. For example, the availability of technically knowledgeable persons to ensure this supervision would be an issue. We were asked to either reword this implementation feature or delete it.

*Response*: We agree that a "knowledgeable" person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, "Authorization and/or supervision," requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis.

*Comment*: The second largest group of comments requested assurance that, with regard to the proposed "Personnel clearance procedure" implementation feature, having appropriate clearances does not mean performing background checks on everyone. We were asked to delete references to "clearance" and use the term "authorization" in its place.

*Response*: We agree with the commenters concerning background checks. This feature was not intended to be interpreted as an absolute requirement for background checks. We retain the use of the term "clearance," however, because we believe that it more accurately conveys the screening process intended than does the term "authorization." We have attempted to clarify our intent in the language of § 164.308(a)(3)(ii)(B), which now reads, "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards. To clarify the intent of this provision, we retitle the implementation specification "Workforce clearance procedure."

*Comment*: One commenter asked that we expand the implementation features to include the identification of the restrictions that should be placed on members of the workforce and others.

*Response*: We have not adopted this comment in the interest of maintaining flexibility as discussed in § 164.306. Restrictions would be dependent upon job responsibilities, the amount and type of supervision required and other factors. We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule (see, for example, § 164.514(d)(2) (relating to minimum necessary requirements), and § 164.530(c) (relating to safeguards).

*Comment*: One commenter believes that the proposed "Personnel security" requirement was reasonable, since an administrative determination of trustworthiness is needed before allowing access to sensitive information. Two commenters asked that we delete the requirement entirely. A number of commenters requested that we delete the implementation features. Another commenter stated that all the implementation features may not be applicable or even appropriate to a given entity and should be so qualified.

*Response*: While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. This final rule has been changed to reflect this approach (see § 164.308(a)(3)(ii)(B)).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 23: Access Termination Policy**

**Introduction**

**PROVIDER COMPLIANCE SOLUTIONS** has adopted this Access Termination Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act “ARRA”) and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

**PROVIDER COMPLIANCE SOLUTIONS** hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information (“IIHI”) generally, and Protected Health Information (“PHI”) as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

**Scope of Policy**

This policy governs the termination of individual access to individually identifiable health information and Protected Health Information for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the termination of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(3).
* Prompt and appropriate termination of workforce member access to individually identifiable health information and Protected Health Information can greatly reduce the likelihood of data breaches and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to terminate any workforce member’s access to individually identifiable health information and Protected Health Information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
* Termination of workforce member access to individually identifiable health information and Protected Health Information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.
* In no case shall the termination of access to individually identifiable health information and Protected Health Information be delayed more than (Insert Time Period – 30 to 60 minutes is recommended, but 24 hours should be the maximum) from the moment of such a triggering event.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all access termination-related activities, in accordance with our Documentation Policy.

**Procedures**

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. ***Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 24: Access Authorization Policy**

**Scope of Policy**

This policy governs the authorization and granting of access to individually identifiable health information and Protected Health Information to workforce members of **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to access authorization, in accordance with the requirements at § 164.308(a)(4).
* The implementation of appropriate processes to grant workforce members access to individually identifiable health information and Protected Health Information can help ensure that our uses and disclosures of individually identifiable health information are lawful and appropriate.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to grant workforce members an appropriate level of access to individually identifiable health information that is based on their work-related duties and responsibilities.
* The level of access to individually identifiable health information and Protected Health Information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all access authorization-related activities and efforts.

**Procedures**

* The billing staff members to all relevant PHI
* Therapists have access to patient information only
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Regulations regarding Access Authorization...**

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. ***Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.**
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 25: Access Establishment and Modification Policy**

**Scope of Policy**

This policy governs establishment and modification of access to individually identifiable health information and Protected Health Information for workforce members of **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and modification of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(4).
* Establishing, maintaining, and modifying appropriate levels of workforce member access to individually identifiable health information and Protected Health Information can help reduce the likelihood of data breaches and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide a lawful and appropriate level of access to individually identifiable health information for each and every workforce member.
* Such access to individually identifiable health information shall be granted based on the nature and duties of the workforce member’s job.
* Higher levels of access shall be provided only to those who need it.
* Any workforce member’s ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all access establishment and modification-related activities and efforts, according to our Documentation Policy.

**Procedures**

* Grant the appropriate level of access to PHI by workforce members as their job requires.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. ***Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 26: Security Reminders Policy**

**Scope of Policy**

This policy governs the creation and implementation of Security Reminders for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to security reminders, in accordance with the requirements at § 164.308(a)(5).
* The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
* The designated HIPAA Official or HIPAA Officer shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all information security reminder-related activities and efforts, according to our Documentation Policy.

**Procedures**

* Set a security reminder on our office calendar
* Periodically review the HHS website
* Periodically search for HIPAA changes online
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

 *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

 *Implementation specifications*. Implement:

1. ***Security reminders* (Addressable). Periodic security updates.**
2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

**HHS Commentaries relevant to Security Reminders...**

**Security Awareness and Training (§ 164.308(a)(5))**

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, **periodic security reminders**, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

**HHS Responses to Comments relevant to Security Reminders**

The amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 27: Malware Protection Policy**

**Scope of Policy**

This policy governs Malware Protection for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
* The use of appropriate techniques, technologies, and methods to protect information systems from malicious software (“malware”) is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
* Responsibility for malware protection shall reside with the designated HIPAA Official or HIPAA Officer, who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from malicious software.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all malware protection-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Use malware, spyware and virus protection etc. on all devices and computers
* Document the specific type pf protection used to protect against viruses, malware, spyware, bots, etc.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

**HIPAA Regulations regarding Malware Protection...**

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

 *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

 *Implementation specifications*. Implement:

1. *Security reminders* (Addressable). Periodic security updates.
2. ***Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.**
3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

**HHS Commentaries regarding Malware Protection...**

**Security Awareness and Training (§ 164.308(a)(5))**

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. **The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 28: Log-In Monitoring Policy**

**Scope of Policy**

This policy governs Log-In Monitoring for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
* Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish a program of regular monitoring and review of log-ins and log-in attempts.
* The HIPAA Official or HIPAA Officer shall assume responsibility for log-in monitoring and analysis, and for ensuring that such activities are executed on a continuous basis.
* Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Assign a username for each user
* Have each user establish a password
* Monitor use on the backend
* Look for discrepancies and abnormal usage
* Address any discrepancies with the user

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

 *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

 *Implementation specifications*. Implement:

1. *Security reminders* (Addressable). Periodic security updates.
2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
3. ***Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.**
4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 29: Password Management Policy**

**Scope of Policy**

This policy governs information systems Password Management for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to password management, in accordance with the requirements at § 164.308(a)(5).
* The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.
* The monitoring of successful and unsuccessful Log-In attempts is a well established method of detecting malicious intrusions, and intrusion attempts, into information systems by unauthorized persons.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to require the use of strong passwords and pass-phrases by all workforce members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information.
* The responsibility for implementing this policy and any attendant procedures is hereby assigned to the designated HIPAA Official or HIPAA Officer, who shall develop and implement this policy in coordination with the most senior information technology personnel.

**Procedures**

* All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of ----- characters in length, and must or should (select one) include non-alphanumeric characters or symbols in them.
* Passwords and pass-phrases must or should be changed by users or management (select one) at least every ------ months.
* In the event of an information system compromise, as determined by the designated HIPAA Official or HIPAA Officer, some or all workforce-member passwords and pass-phrases may need to be changed. This determination shall be made by the designated HIPAA Official or HIPAA Officer (or insert alternate contact).
* Under no circumstances shall passwords or pass-phrases be written down and kept at or near computers and workstations where they may be found by others. Passwords and pass-phrases may, however, be written down and stored in a workforce member’s wallet or purse, if the password or pass-phrase is thus afforded protection equal to the protection afforded to workforce members’ cash, credit cards, and other critical documents.
* Any workforce member who loses, misplaces, forgets, or experiences any compromise of their password or pass-phrase shall immediately notify the designated HIPAA Official or HIPAA Officer, or, if they are unavailable, shall notify (specify alternate notification contact). Such notification of password or pass-phrase compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one (1) (Choose or select alternate number) hour(s).
* Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by this organization.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

 *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

 *Implementation specifications*. Implement:

1. *Security reminders* (Addressable). Periodic security updates.
2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
4. ***Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.**

**Security Awareness and Training (§ 164.308(a)(5))**

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, **and user education in password management**.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 30: Policy on Security Incident Procedures**

**Scope of Policy**

This policy governs responses to Security Incidents involving the breach or compromise of Protected Health Information for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
* Appropriate responses to security incidents may include, but are not limited to:
	+ Rapid identification and classification of the severity of security incidents.
	+ Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
	+ Repairing, patching, or otherwise correcting the condition or error that created the security incident.
	+ Retrieving or limiting the dissemination of individually identifiable health information, if possible.
	+ Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
	+ Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to:
		- Patients
		- Consumers
		- Regulatory Authorities, including HHS and/or the Federal Trade Commission
		- Law Enforcement
		- The local media, if necessary and required by law
	+ Mitigating any harmful effects of the security incident.
	+ Fully documenting security incidents, along with their causes and our responses.
	+ Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
* Compliance with HIPAA’s data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
* Responsibility for responding to and managing security incidents shall reside with the designated HIPAA Official or HIPAA Officer (or specify other responsible party).
* The designated HIPAA Official or HIPAA Officer or, specify other responsible party shall develop specific forms and procedures that shall be implemented in response to security incidents.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

**Procedures**

* List specific security incident procedures in this section.
* List specific security incident procedures in this section.
* List specific security incident procedures in this section.
* List specific security incident procedures in this section.
* List specific security incident procedures in this section.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

*6.) Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

*Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

**Security Incident Procedures (§ 164.308(a)(6))**

We proposed a requirement for implementation of accurate and current **security incident procedures**: formal, documented report and response procedures so that security violations would be reported and handled promptly. We adopt this standard in the final rule, along with an implementation specification for response and reporting, since documenting and reporting incidents, as well as responding to incidents are an integral part of a security program.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 31: Data Backup Policy**

**Scope of Policy**

This policy governs Data Backups for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backups, in accordance with the requirements at § 164.308(a)(7) and elsewhere in the Regulations.
* The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
* The storage of data backups in a separate location, removed from our normal business operations (“offsite”) is an essential element of any successful data backup plan.
* Timely access to health information is crucial to providing high quality health care, and to our business operations.
* Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
* No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
* A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
* All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times.

**Procedures**

* **Name of Responsible Party or Person** is responsible for performing daily backups on **PROVIDER COMPLIANCE SOLUTIONS**’s network, including shared drives containing application data, patient information, financial data, and crucial system information.
* **PROVIDER COMPLIANCE SOLUTIONS** will back up all such data automatically, per **Name of Backup Solution**’s programmed standards, nightly at 2300 hours.
* **Name of Responsible Party or Person,** or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in **Location of Backup Vault or Facility**.
* The media vault meets fire and disaster standards for media and will be kept locked at all times. Only the **Name of Responsible Party or Person**, the system administrator, and their designees have access to the media vault.
* In the event that the secured media vault is not available or properly functioning, the **Name of Responsible Party or Person**, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
* **Name of Responsible Party or Person**, the system administrator, or their designees will use **Name of Backup Solution**’s reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
* Individuals so validating the backup will generate daily reports and log them in the network log in the system administrator’s office. The system administrator will maintain such reports for a minimum of 30 days (or specify other number of days, weeks, or months).
* Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
* Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer’s recommended guidelines, currently once per week (or specify other period).
* A rotation of four, or specify other number weekly data tapes must be maintained at all times.
* **Name of Responsible Party or Person** will ensure replacement of backup tapes or media according to manufacturer’s recommended guidelines, currently annually (or specify other media replacement timeframe(s)).
* The **Name of Responsible Party or Person** is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly (or specify other period) and more often if necessary to ensure data integrity, availability, and confidentiality.
* Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
* All personnel who detect or suspect a data backup problem should immediately report the same to the **Name of Responsible Party or Person**. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
	+ Narrative of the data backup problem.
	+ How long the problem has existed.
	+ Suggested solutions.

**Compliance and Enforcement**

All information technology managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
	1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
	2. *Implementation specifications*:
		1. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		2. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		3. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		4. ***Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 32: Disaster Recovery Policy**

**Scope of Policy**

This policy governs contingency Disaster Recovery Planning for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).
* HIPAA requires **PROVIDER COMPLIANCE SOLUTIONS** to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information.
* A disaster may occur at any time, not necessarily during work hours.
* **PROVIDER COMPLIANCE SOLUTIONS** must remain operational with as little disruption of business operations and patient care as possible.
* Continuity of patient care requires uninterrupted access to patient information.
* In a dangerous emergency, evacuating personnel has priority over preserving information assets.
* The following conditions can destroy or disrupt **PROVIDER COMPLIANCE SOLUTIONS**’s information systems:
	+ Power interruption.
	+ Fire.
	+ Water.
	+ Weather and other natural phenomena, such as earthquakes.
	+ Sabotage and vandalism.
	+ Terrorism.

**Policy Statement**

It is the policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information.

**Procedures**

**Preventive** **Measures**

* **Name of Responsible Party or Person** and or their designee(s) shall ensure that the following preventive measures, as applicable, are implemented and documented:
	+ Retain dictation on disk for three months (or specify other time period).
	+ Back up computerized files according to our Data Backup Policy.
	+ Store backup media tape in the off-site media vault, according to our Data Backup Policy.
	+ Maintain and replace backup tapes according to our Data Backup Policy.
	+ Test integrity of backup system no less than monthly (or specify other time period), according to our Data Backup Policy.
	+ Store media properly. For example, laser discs must be stored in sleeves of plastic, paper, or combination of the two, placed in cardboard jackets or boxes, and stored on edge on metal shelving, properly labeled.
	+ Color-code all media as to priority of evacuation: red is first priority; yellow is second priority; green is third priority.
	+ Protect by uninterruptible power supplies all servers and other critical equipment from damage in the event of an electrical outage.
	+ Locate file servers and other critical hardware in rooms with Halon fire protection systems which limit damage to the immediate area of the fire. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
	+ In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
	+ In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
	+ Training in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster.
* **Name of Responsible Party or Person** must implement and document the following:
	+ Ensure that major hardware is covered under **PROVIDER COMPLIANCE SOLUTIONS**’s property and casualty, and or other appropriate insurance policy or policies.
	+ Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

**Priority Tasks during Emergencies**

As applicable, and under appropriate circumstances, all workforce members should:

* + Remain calm.
	+ Activate the alarm. That is, pull the fire alarm or call 911 as appropriate.
	+ Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
	+ If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
	+ If safe, close all doors as you leave.
	+ Obtain portable phone(s) to communicate.
	+ Notify concerned fire, police, security, administration, and others as necessary.
	+ Notify other departments of situation and emergency protocols.
	+ If computers have not automatically powered down, initiate procedures to orderly shut down systems, when possible.
	+ If a fire or flood occurs, disconnect power if possible.
	+ If a fire or flood occurs, try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
	+ Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
	+ Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
	+ Respond to requests for records via portable phone rather than computer.
	+ Continue to provide patient charts as requested by physicians or other parties.

**Priority Disaster Recovery Tasks**

As applicable, and under appropriate circumstances, all workforce members should:

* + Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
	+ Not permit unauthorized personnel to enter the affected area.
	+ Determine the extent of the damage and whether additional equipment/supplies are needed.
	+ Determine how long it will be before service can be restored, and notify departments.
	+ Replace hardware as necessary to restore service.
	+ Work with vendors as necessary to ensure that support is given to restore service.
	+ Notify insurance carriers.
	+ Retrieve and upload backup files if necessary to restore service.
	+ Air-dry floppy disks, if any, using a hair dryer on “air,” not “heat.” When dry, copy disk.
	+ For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
	+ Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
	+ Wrap paper records to prevent them from sticking together. Label the wrapped records.
	+ Contact fire, water, and storm damage restoration company. Contract for services as needed.
	+ Reconstruct/reacquire documents from the following:
		- Dictation system.
		- Word processing system.
		- Computer system.
		- Holders of document copies.
	+ Move records and equipment back to home location.
	+ Catch up on filing.
	+ Ensure that backup procedures are followed.
	+ Document data that cannot be recovered in patient record.
	+ Meet with management and staff to identify opportunities for improvement.

**Additional Disaster Recovery Tasks**

The following tasks must be assigned to specific persons or positions:

* Determine whether additional equipment and supplies are needed.
* Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
* If necessary, check with other vendors to see whether they can provide faster delivery.
* Rush order any supplies and equipment necessary.
* Notify personnel that an alternate site will be necessary and where it is located.
* Coordinate moving equipment and support personnel to the alternate site.
* Bring recovery materials from offsite storage to the alternate site.
* As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
* Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
* Prepare backup materials and return them to the offsite storage area.
* Set up operations at the alternate site if necessary.
* Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
* Ensure that periodic backup procedures are followed according to our Data Backup Policy.
* Plan to phase in all critical support.
* Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
* Coordinate with administration and others for continuing support and ultimate restoration of normal operations.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	4. 1. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
		2. *Implementation specifications*. Implement:
			1. *Security reminders* (Addressable). Periodic security updates.
			2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
			3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
			4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.
		3. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
		4. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
	5. 1. ***Standard: Contingency plan*.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
		2. *Implementation specifications*:
			1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
			2. ***Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.**
			3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
			4. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
			5. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 33: Emergency Mode Operations Policy**

**Scope of Policy**

This policy governs Emergency Mode Operations and planning for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).
* Individually identifiable health information must be protected during emergencies, even as it is protected during normal operations. This Emergency Mode Operations Policy is designed to ensure the protection and availability of individually identifiable health information and Protected Health Information during emergencies requiring **PROVIDER COMPLIANCE SOLUTIONS** to operate in “emergency mode”.
* Our Emergency Mode Operations Plan must be implemented and executed in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish this Emergency Mode Operations Policy to implement procedures to enable continuation of critical business processes for the protection of individually identifiable health information while operating in emergency mode.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.
* Our Emergency Mode Operations Plan shall be executed whenever **PROVIDER COMPLIANCE SOLUTIONS** must operate in “emergency mode”.
* “Emergency Mode” shall be in effect and activated whenever one or more of the following conditions applies:
	+ Electrical power is unavailable for more than eight (or specify other number) hours.
	+ Fire, flood, storm or other natural disaster renders our normal business facility unavailable or unusable for more than eight (or specify other number) hours.
	+ Any other condition renders our normal business facility unavailable or unusable for more than eight (or specify other number) hours.

**Procedures**

***Responsibility and Role Assignments***

The following personnel are hereby assigned to lead the functions listed below during emergency mode operations...

|  |  |
| --- | --- |
| **Function** | **Individual(s) Assigned** |
| **Telephones Outbound** |  |
| **Telephones Inbound** |  |
| **Computing Resources** |  |
| **U.S. Mail** |  |
| **Couriers (FedEx, etc.)**  |  |
| **Internet and Email** |  |
| **Customer/Patient Contact** |  |
| **Medical Records** |  |
| **Other Business Records** |  |
| **Legal Issues** |  |
| **Transportation** |  |
| **Internal Communications** |  |
| **Physical Security** |  |
| **Utilities Restoration** |  |
| **Remediation & Restoration** |  |
| **Vendor/Partner Relations** |  |
| **Media Relations** |  |

***Additional Emergency Mode Operations Procedures***

* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	4. 1. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
		2. *Implementation specifications*. Implement:
			1. *Security reminders* (Addressable). Periodic security updates.
			2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
			3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
			4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.
		3. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
		4. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
	5. 1. ***Standard: Contingency plan*.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
		2. *Implementation specifications*:
			1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
			2. ***Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.**
			3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
			4. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
			5. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 34: Testing and Revision of**

**Contingency and Emergency Plans and Procedures**

**Scope of Policy**

This policy governs Testing and Revision of Contingency and Emergency Plans and Procedures for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).
* Emergency and contingency plans, and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of **PROVIDER COMPLIANCE SOLUTIONS**.
* Individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to periodically test, and revise as necessary, all emergency preparedness plans, including emergency and contingency plans.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** that all individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

**Procedures**

* Emergency and contingency plans are the responsibility of the designated HIPAA Official or HIPAA Officer, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
* Emergency and contingency plans shall be reviewed, and revised if necessary, at least annually (or specify other time period). Copies of all such plans shall remain on file and be available to all personnel.
* Emergency and contingency plans shall be rehearsed, with all team members participating in such rehearsals, at least twice annually (or specify other time period).
* The designated HIPAA Official or HIPAA Officer shall fully document all emergency preparedness plans, including emergency and contingency plans, and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	4. 1. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
		2. *Implementation specifications*. Implement:
			1. *Security reminders* (Addressable). Periodic security updates.
			2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
			3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
			4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.
		3. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
		4. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
	5. 1. ***Standard: Contingency plan*.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
		2. *Implementation specifications*:
			1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
			2. ***Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.**
			3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
			4. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
			5. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy on Data and Applications**

**Criticality Analyses**

**Scope of Policy**

This policy governs Data and Applications Criticality Analyses for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
* A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) during emergencies and during normal business operations.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

**Procedures**

* Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* Criticality analysis shall be the responsibility of Name of Responsible Party or Person, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
* Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that **PROVIDER COMPLIANCE SOLUTIONS** possesses and/or uses to the continuity and success of our operations.
* The most critical data and applications shall be given the given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
* In conducting data and applications analyses, Name of Responsible Party or Person shall employ the technical guidance and recommendations of the National Institute of Standards and Technology (“NIST”), and/or other information technology “best practices”, as appropriate.
* Name of Responsible Party or Person shall fully document all analyses of the relative criticality of both data and applications, in accordance with our Documentation Policy and the requirements of HIPAA.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	4. 1. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
		2. *Implementation specifications*. Implement:
			1. *Security reminders* (Addressable). Periodic security updates.
			2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
			3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
			4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.
		3. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
		4. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
	5. 1. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
		2. *Implementation specifications*:
			1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
			2. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
			3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
			4. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
			5. ***Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy on Evaluating the Effectiveness of**

**Security Policies and Procedures**

**Scope of Policy**

This policy governs periodic Evaluations of the Effectiveness of Security Policies and Procedures for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
* Security policies and procedures, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to periodically evaluate security policies and procedures, including emergency and contingency plans and procedures, in order to improve their effectiveness.

**Procedures**

* It shall be the responsibility of Name of Responsible Party or Person to periodically conduct such technical and nontechnical evaluations.
* Name of Responsible Party or Person shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
* Such technical and nontechnical evaluations shall be conducted at least every six months (or specify another timeframe).
* The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.
* The purpose of such evaluations is to improve the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) that we possess or use.
* Name of Responsible Party or Person shall fully document our periodic technical and nontechnical evaluations to determine the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, in accordance with our Documentation Policy and the requirements of HIPAA.
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:
	* 1. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.
		2. *Implementation specifications*:
			1. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
			2. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
			3. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
			4. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	1. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
	2. 1. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
		2. *Implementation specifications*:
			1. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
			2. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
			3. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
	3. 1. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
		2. *Implementation specifications*:
			1. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
			2. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
			3. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	4. 1. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).
		2. *Implementation specifications*. Implement:
			1. *Security reminders* (Addressable). Periodic security updates.
			2. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
			3. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
			4. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.
		3. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.
		4. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
	5. 1. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
		2. *Implementation specifications*:
			1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
			2. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
			3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
			4. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.
			5. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.
	6. ***Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**

**Evaluation (§ 164.308(a)(8))**

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 37: Business Associates Policy**

**Scope of Policy**

This policy governs relationships with, and operations involving Business Associates for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to Business Associates, in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.
* In cooperation with our organization, Business Associates work with, use, transmit, and/or receive individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), which is afforded specific protections under HIPAA.
* **PROVIDER COMPLIANCE SOLUTIONS** has the primary responsibility in all Business Associate relationships to ensure that individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), is properly protected and safeguarded.
* The HIPAA (“Omnibus”)Final Rule specifically identifies the following types of entities as business associates:
	+ Subcontractors.
	+ Patient safety organizations.
	+ HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
	+ E-Prescribing gateways.
	+ PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
	+ Other firms or persons who “facilitate data transmission" that requires routine access to PHI.
* The “Minimum Necessary Standard” now applies directly to Business Associates. HIPAA now applies the Minimum Necessary standard directly to Business Associates and their subcontractors. When using, disclosing or requesting PHI, all these entities must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
* Subcontractors of Business Associates are now Business Associates themselves. A subcontractor is defined as a person or entity to whom a Business Associate delegates a function, activity, or service involving Protected Health Information, and who is not a member of the Business Associate’s own workforce.
* **PROVIDER COMPLIANCE SOLUTIONS** is not required to enter into a contract or other arrangement with a Business Associate that is a subcontractor. That is the responsibility of the primary or first-tier Business Associate.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain business and working relationships with Business Associates that are in full compliance with all the requirements of HIPAA Final “Omnibus” Rule.

**Procedures**

* Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the designated HIPAA Official or HIPAA Officer, who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
* With regard to Business Associates, the duties and responsibilities of the designated HIPAA Official or HIPAA Officer shall include, but are not limited to the following:
	+ Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA “Omnibus” Final Rule, and any requirements of State laws in the state(s) where we operate.
	+ Ensure that individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
	+ Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), whether in electronic form (“ePHI”) or hardcopy form.
	+ Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), before entrusting such information to them.
	+ Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
	+ The designated HIPAA Official or HIPAA Officer shall fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy and the requirements of HIPAA.
	+ < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Administrative Safeguards - § 164.308** |

1. A covered entity or business associate must, in accordance with § 164.306:

S*tandard: Business associate contracts and other arrangements*. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

*Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

*Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

**Business Associate Contracts or Other Arrangements (§ 164.308(b)(1))**

In the proposed rule § 142.308(a)(2) "Chain of trust" requirement, we proposed that covered entities be required to enter into a chain of trust partner agreement with their business partners, in which the partners would agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged. This standard has been modified from the proposed requirement to reflect, in § 164.308(b)(1) "Business associate contracts and other arrangements," the business associate structure put in place by the Privacy Rule.

In this final rule, covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see § 164.314(a)(1)).

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Organizational Requirements - § 164.314** |

a.

1. *Standard: Business associate contracts or other arrangements*. The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.
2. *Implementation specifications (Required)*.
	1. *Business associate contracts*. The contract must provide that the business associate will--
		1. Comply with the applicable requirements of this subpart;
		2. In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
		3. Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.
	2. *Other arrangements*. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).
	3. *Business associate contracts with subcontractors*. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

**NOTE:**

BA = Business Associate

CE = Covered Entity

The Omnibus Rule expands the definition of a “business associate” to generally include all those entities that create, receive, maintain, or transmit PHI on behalf of a CE.

BAs under the Final Rule provide certain identified services *involving PHI* (rather than just IIHI).

The Final Rule also specifically identifies the following types of entities as business associates:

1. Subcontractors.
2. Patient safety organizations.
3. HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
4. E-Prescribing gateways.
5. PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that *do not* offer PHRs on behalf of CEs are *not* BAs.
6. Other firms or persons who “facilitate data transmission" that requires routine access to PHI.

BAs (including their subcontractors) now are subject to civil money penalties and other enforcement actions for noncompliance. Like CEs, BAs may also be liable for violations by their agents.

**Timeline of Business Associate Obligations under HIPAA**



**Minimum Necessary Standard Now Applies Directly to BAs**

The Omnibus Rule applies the “minimum necessary” standard directly to BAs and their subcontractors. When using, disclosing or requesting PHI, all these entities must “make reasonable efforts to limit [the PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”

**BA Subcontractors**

Subcontractors of business associates are now the same category as business associates, in the compliance sense.

Subcontractor + PHI = Business Associate!

The Omnibus Rule pulls subcontractors into the definition of business associates. Under the Omnibus Rule, a subcontractor is defined as a person or entity to whom a BA delegates a function, activity, or service, and who is *not* a member of the BA’s workforce.

This means that a subcontractor of a BA that creates, receives, maintains, or transmits PHI on behalf of the first or primary BA, is now itself a BA and subject to the HIPAA provisions applicable to BAs.

The Omnibus Rule did not change the definition of business associate, but instead simply adds subcontractors to the list of entities that are included as BAs.

Therefore, the business associate who contracts with the covered entity, the business associate’s subcontractor, and any subcontractor of a subcontractor—all the way down the chain – are business associates to the extent they create, receive, maintain, or transmit PHI.

**The CE-BA Chain**



The Omnibus Rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a BA that is a subcontractor—that is the responsibility of the primary or first tier BA.

**Q -- When is a Subcontractor *not* a BA?**

**A --** **When a subcontractor is assisting with a BA’s *own* management, administration, or legal responsibilities.** The BA still must obtain reasonable assurances of confidentiality from the subcontractor, plus assurance of notification from the subcontractor in case of breach, loss, or compromise of data.

**Who is *not* a BA?**

* Health Care Providers (for treatment purposes)
* Health Plan Sponsors (for plan sponsor activities after plan amendments and certifications)
* Government Agencies (for determining eligibility for or enrollment in a government health plan)
* Covered Entities that participate in an OHCA (for functions on behalf of the OHCA)
* External Researchers (for research activities)
* IRBs (in performing research review, approval, and continuing oversight)
* Financial institutions (for cashing checks or conducting funds transfer)
	+ Subject to the Section 1179 exemption
* Onsite Contractors (when treated as workforce)
* Medical Liability Insurers (when CE purchases a health plan product or other insurance)

**The Business Associate Conduit Exception**

HHS reiterated that the definition of a BA does not include “conduits” who:

1. Transport PHI; and,
2. Do not access PHI other than on a random or infrequent basis to support transport or as required by law.

The Conduit Exception:

* Is limited to transmission services (whether digital or hard copy), including temporary storage incident to transmission
* Does not include an entity that maintains PHI on behalf of a covered entity, e.g., digital or hard copy “document storage companies”

It does not matter whether the entity maintaining the PHI actually views the PHI. And HHS did not address whether entity with only encrypted information (and without key) is a BA.

The Conduit Exception includes:

* U.S. Postal Service, FedEx, UPS, etc.
* ISPs who merely provide data transmission services

**BA Direct Liability**

The Omnibus Rule makes business associates directly liable for compliance with many of the same standards and implementation specifications under the security rule and applies the same penalties to business associates that apply to covered entities.

Under the privacy rule, business associates may use or disclose PHI only in accordance with their business associate contracts or as required by law. Moreover, a business associate may not use or disclose PHI in a manner prohibited by the privacy rule if done by a covered entity (unless HIPAA specifically permits such use and disclosure for business associates). A BA may only use or disclose information in the same manner as the CE. Therefore, any Privacy Rule limitations on how a CE uses or discloses PHI automatically extend to a business associate, and create direct liability for the BA.

The Final Rule adopted the proposal to apply the Minimum Necessary standard directly to BAs when using or disclosing PHI, or when requesting PHI from another CE. It is up to the discretion of the contracting parties to determine to what extent the BA Agreement will include specific Minimum Necessary provisions. HHS intends to issue further guidance on the Minimum Necessary standard with respect to BAs.

Not all of the requirements of the Privacy Rule apply to business associates.

For example, business associates do not need to provide a notice of privacy practices or designate a privacy official (unless the covered entity has chosen to delegate such a responsibility to the business associate, which then would make it a contractual requirement for which contractual liability would attach).

Furthermore, BAs must obtain “satisfactory assurances” in the form of business associate contracts from their subcontractor business associates. Finally, business associates must furnish any information that HHS requires to investigate whether the business associate is in compliance with the regulations.

**BAs are Directly Liable under HIPAA for the Following:**

1. Impermissible uses and disclosures;
2. Failure to provide breach notification to the CE;
3. Failure to provide access to a copy of electronic PHI to either the CE, the individual, or the individual’s designee (whichever is specified in the BAA);
4. Failure to disclose PHI where required by HHS to investigate or determine the business
5. BA’s general, overall compliance with HIPAA, as required;
6. Failure to provide an accounting of disclosures; and
7. Failure to comply with the applicable requirements of the Security Rule.

**BA Duties under HIPAA Fall into Four General Categories....**

1. **Required by HIPAA (penalties for noncompliance)**
	* Limit uses and disclosures of PHI
		1. Pursuant to HIPAA
		2. Pursuant to BAA
	* Notify CE or upstream BA of breach of unsecured PHI.
	* Provide electronic copy of designated record set to CE, upstream BA, or individual (as set forth in BAA) to respond to request for access.
	* Disclose records (including PHI) to HHS for HHS HIPAA investigation.
	* Provide an accounting of disclosures.
	* Comply with the Security Rule
		1. General requirements
		2. Administrative safeguards
		3. Physical safeguards
		4. Technical safeguards
		5. Organizational requirements
		6. Policies and documentation
2. **Required Only by BA Agreement (Non-compliance = Breach of Contract)**
* Safeguards for hard copy and verbal PHI
* Report impermissible uses and disclosures that do not qualify as a breach of unsecured PHI
* Report security incidents
* Provide designated record set maintained in hard copy to respond to request for access
* Ensure that appropriate agreement is in place with subcontractors (potentially punishable impermissible disclosure)
* Make available PHI for amendments and incorporate amendments
* Return or destroy PHI at termination
1. **Potential “Best Practices”**
* Designate a privacy official
* Policies and procedures governing privacy (use, disclosure, access, amendment, accounting)
* Training on privacy
* Sanctions policy for privacy noncompliance
* Document retention policy for privacy
* Encrypt all data received, used, stored or transmitted
1. **Not Required Unless Delegated (in writing, in the BAA)**
* HIPAA-compliant Notice of Privacy Practices
* Complaint process

**BA Agreements**

The Omnibus Rule includes up to a one-year extension for CEs and BAs to revise their BA Agreements, if such agreements were entered into and compliant with HIPAA as of Jan. 25, 2013 (the date of the Omnibus Rule publication in the Federal Register).

BA Agreements (BAAs) must establish uses and disclosures of PHI:

* As Required by HIPAA.
* As Permitted by HIPAA.

**New and Renewed BA Agreements - Timing Options**

If the parties to a BAA had a HIPAA-compliant Agreement in place before January 25, 2013, and the BAA is *not renewed* between March 26, 2013 and September 2013, then they can continue to lawfully use that BAA until September 23, 2014.

If the parties to a BAA *did not* have a HIPAA-compliant Agreement in place by January 25, 2013, then they must enter into a compliant BAA by September 23, 2013 – one year earlier than for grandfathered BAAs.

No matter what, if a BAA is renewed between September 23, 2013 and September 23, 2014, the new BAA must comply with the HIPAA Final (Omnibus) Rule.

The Omnibus Rule makes BA contracts applicable to arrangements involving a business associate and a subcontractor of that business associate in the same manner that business associate contracts apply to arrangements between a covered entity and its direct business associate. If a subcontractor creates, receives, maintains, or transmits PHI, then a BA must have a BAA with the subcontractor.

HHS emphasizes the continued need for BA contracts even though BAs now are held directly accountable for many provisions of HIPAA. HHS notes that BAA are necessary to clarify and limit permissible uses and disclosures of PHI, ensure business associates are contractually responsible for activities for which they are not directly liable under HIPAA, and clarify respective responsibilities related to patient rights, such as access to PHI.

Each agreement in the BA contract chain must be as or more stringent than the one above it regarding the uses and disclosures of PHI.

**“Patterns of Activity” and HIPAA BA Compliance Status**

A CE or BA is not in compliance with Business Associate obligations:

* If it knew of a pattern of activity, or practice of its business associate or subcontractor that constituted a material breach or violation of BA’s or subcontractor’s obligation(s);
* Unless it takes reasonable steps to cure the breach or end the violation; and if unsuccessful, terminates the arrangement, if feasible (No requirement to notify HHS).

**BAs of Health Plans and Limited Data Sets**

If *only* a limited data set is disclosed to a BA of a health plan for health care operations, only a data use agreement is required and a BA Agreement is *not* required.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 39: Facility Security Policy**

**Scope of Policy**

This policy governs Facility Security for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Presumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a)(1-2).
* In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.

**Procedures**

* Primary responsibility for facility security is hereby assigned to Name of Responsible Party or Person, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
* The analyses of our facility security should include, but are not limited to, the following factors:
	+ Windows and doors
	+ Roofs and the potential for roof access
	+ Locks and keys
	+ Electronic access control systems
	+ Video cameras and video surveillance systems
	+ Electronic alarms and related systems
	+ Employee, partner, vendor and guest access
	+ Vehicle parking security
	+ Routine and non-routine deliveries
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. **Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.**
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Access Control and Validation Policy**

**Scope of Policy**

This policy governs Access Control and Validation for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to access control and validation, in accordance with the requirements at § 164.310(a)(1-2).
* Access control and validation procedures are designed to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.
* Strong access control and validation procedures are an essential element of protecting individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to implement and support strong and ongoing access control and validation procedures, in full compliance with all the requirements of HIPAA.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document access control and validation procedures, in accordance with our Documentation Policy.

**Procedures**

* Responsibility for developing, testing, analyzing, and periodically updating access control and validation procedures shall reside with Name of Responsible Party or Person.
* The development and implementation of specific access control and validation procedures shall be conducted in accordance with guidance and information provided by the National Institute of Standards and Technology (“NIST”), or other information technology “best practices”.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

**Facility Access Controls (§ 164.310(a)(1))**

We proposed, under the "Physical access controls" requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

**In § 164.310(a)(2), we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**40: Facility Security Maintenance Records Policy**

**Scope of Policy**

This policy governs the disposition of records pertaining to maintenance of the physical security of **PROVIDER COMPLIANCE SOLUTIONS**’s facilities. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security maintenance records, in accordance with the requirements at § 164.310(a)(1-2).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
* Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Responsibility for the creation and updating of facility security maintenance records is hereby assigned to Name of Responsible Party or Person, who shall establish procedures for maintaining such records in appropriate form.
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. ***Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)**.

**Facility Access Controls (§ 164.310(a)(1))**

We proposed, under the "Physical access controls" requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, **maintenance records**, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

**In § 164.310(a)(2), we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 42: Workstation Use Policy**

**Scope of Policy**

This policy governs Information Workstation Use for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
* The establishment and implementation of an effective workstation use policy is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to configure, operate, and maintain our information workstations in full compliance with all the requirements of HIPAA.
* Our objective in these efforts is to providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

**Procedures**

* Responsibility for the development and implementation of this workstation use policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* < List specific workstation use procedures in this section >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. ***Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.**
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

**Workstation Use (§ 164.310(b))**

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

**Workstation Security (§ 164.310(c))**

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 43: Workstation Security Policy**

**Scope of Policy**

This policy governs Workstation Security for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
* The establishment and implementation of an effective workstation security policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain this workstation security policy in full compliance with all the requirements of HIPAA.
* Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), to restrict access to authorized users only.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Log off before leaving you're a work station
* Turn all devices away from unauthorized users
* Use screen protectors when necessary

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. ***Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**

**Workstation Use (§ 164.310(b))**

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

**Workstation Security (§ 164.310(c))**

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 44: Media Disposal Policy**

**Scope of Policy**

This policy governs Media Disposal for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
* Media containing individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to dispose of all media containing individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), in full compliance with all the requirements of HIPAA.
* Responsibility for proper media disposal and disposition shall reside with Name of Responsible Party or Person, who shall develop procedures to ensure the proper disposition of all such media.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* < List specific media disposal and disposition procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
	1. ***Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**
	2. ***Implementation specifications*:**
		1. ***Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.**
		2. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		3. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		4. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 45: Media Re-Use Policy**

**Scope of Policy**

This policy governs the Re-Use of Information Storage Media for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
* Media containing individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), must be completely erased or sanitized (“wiped”) before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to properly erase and or sanitize (“wipe”) all media containing individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), before any media may be re-used.
* Responsibility for proper media re-use shall reside with Name of Responsible Party or Person, who shall develop procedures to ensure the proper disposition of all such media before any re-use.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* < List specific media re-use procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
	1. ***Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**
	2. *Implementation specifications*:
		1. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		2. ***Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.**
		3. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		4. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**46: Hardware and Media Accountability Policy**

**Scope of Policy**

This policy governs the Accountability of Information Systems Hardware and Media for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at § 164.310(d)(1-2).
* Proper protection of individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA), requires that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
* Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to ensure that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all hardware and media accountability-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* < List specific hardware and media accountability procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
	1. ***Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**
	2. *Implementation specifications*:
		1. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		2. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		3. ***Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.**
		4. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 47: Data Backup and Storage Policy**

**Scope of Policy**

This policy governs Data Backup and Storage for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to data backup and storage, in accordance with the requirements at § 164.310(d)(1-2) and § 164.308(a)(7).
* The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and electronic protected health information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
* The storage of data backups in a separate location, removed from our normal business operations (“offsite”) is an essential element of any successful data backup plan.
* Timely access to health information is crucial to providing high quality health care, and to our business operations.
* Physicians and others must have immediate, around-the-clock access to patient information.
* No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
* A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to create retrievable, exact copies of electronic protected health information, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.
* The Name of Responsible Party or Person is responsible for performing appropriate backups on **PROVIDER COMPLIANCE SOLUTIONS**’s network, including shared drives containing application data, patient information, financial data, and crucial system information.

**Procedures**

* Name of Responsible Party or Person will back up all such data as necessary, per Name of Backup Solution ’s programmed standards, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information..
* The Name of Responsible Party or Person or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in Location of Backup Vault or Facility.
* The media vault meets fire and disaster standards for media and will be kept locked at all times. Only Name of Responsible Party or Person, the system administrator, and their designees have access to the media vault.
* In the event that the secured media vault is not available or properly functioning, Name of Responsible Party or Person, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
* Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
* Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer’s recommended guidelines, currently once per week, or specify other period.
* The Name of Responsible Party or Person will ensure replacement of backup tapes or media according to manufacturer’s recommended guidelines, currently annually (or specify other media replacement timeframe(s)).
* The Name of Responsible Party or Person is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly(or specify other timeframe), and more often if necessary to ensure data integrity, availability, and confidentiality.
* Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
* All personnel who detect or suspect a data backup problem should immediately report the same to the Name of Responsible Party or Person. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
	+ Narrative of the data backup problem.
	+ How long the problem has existed.
	+ Suggested solutions.
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >
* < Add specific procedure here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Physical Safeguards - § 164.310** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
	2. *Implementation specifications*:
		1. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		2. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		3. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		4. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
1. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
2. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
	1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
	2. *Implementation specifications*:
		1. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		2. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		3. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		4. ***Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.**

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 48: Unique User I.D. Policy**

**Scope of Policy**

This policy governs the issuance, maintenance, and security of Unique User I.D.’s for access to **PROVIDER COMPLIANCE SOLUTIONS**’s information systems. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of unique user I.D.’s, in accordance with the requirements at § 164.306, and § 164.312(a)(1).
* The use of unique user I.D.’s is an essential element in our overall effort to protect individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to exclusively use unique user I.D.’s for all information system access and activities, in full compliance with all the requirements of HIPAA.
* Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.’s.
* Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Issue a unique user identifier for all personnel for electronic devices
* All personnel shall use a password to protect the ePHI
* User ID’s and passwords shall be removed as soon as the user is terminated or resigns.
* An emergency user name and password will be established for all personnel.
* All user names will automatically log off after 1 minutes of non-use.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. ***Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).**
	2. ***Implementation specifications*:**
		1. ***Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.**
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

**Access Control (§ 164.312(a)(1))**

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

**Audit Controls (§ 164.312(b))**

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

**Integrity (§ 164.312(c)(1))**

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

**Person or Entity Authentication (§ 164.312(d))**

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone callback," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 49: Emergency Access Policy**

**Scope of Policy**

This policy governs Access to Protected Health Information during emergencies for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency access procedures, in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).
* The establishment of emergency access procedures further strengthens the protections we offer to individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
* These emergency access procedures apply to access to individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* Responsibility for the development and implementation of our emergency access procedures shall reside with Name of Responsible Party or Person, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) during emergencies.
* These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document our emergency access procedures development and implementation, in accordance with our Documentation Policy and the requirements of HIPAA.

**Procedures**

* Assign a unique user ID for all each user.
* Maintain an emergency password for each user ID.
* Each electronic device shall have an auto logoff after 1 minutes of non-use.
* ePHI shall be stored in encrypted files and folder or devices.

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

**Access Control (§ 164.312(a)(1))**

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control.

In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 50: Automatic Log-Off Policy**

**Scope of Policy**

This policy governs the implementation of Automatic Log-Offs for **PROVIDER COMPLIANCE SOLUTIONS**’s information systems. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of automatic log-off applications, in accordance with the requirements at § 164.306 and § 164.312(a)(1-2).
* The establishment and implementation of an effective automatic log-off policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to always use automatic log-off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.
* Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document automatic log-off-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Auto log-off must be enabled on all electronic devices.
* < List specific automatic log-off procedures here >
* < List specific automatic log-off procedures here >
* < List specific automatic log-off procedures here >
* < List specific automatic log-off procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. ***Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.**
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

**Access Control (§ 164.312(a)(1))**

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

**Audit Controls (§ 164.312(b))**

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

**Integrity (§ 164.312(c)(1))**

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

**Person or Entity Authentication (§ 164.312(d))**

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone callback," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1). "Automatic logoff" has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Policy 51: Encryption and Decryption Policy**

**Scope of Policy**

This policy governs the Encryption and Decryption of Protected Health Information for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
* The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
* Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Use encrypted devices and files for all ePHI.
* Maintain a unique user ID for all users.
* Use auto log-off on all electronic devices.
* < List specific encryption and decryption procedures here >
* < List specific encryption and decryption procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. ***Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).**
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. ***Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.**

**Access Control (§ 164.312(a)(1))**

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

**Transmission Security (§ 164.312(e)(1))**

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**52: Audit Controls Policy**

**Scope of Policy**

This policy governs Audit Controls for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).
* The establishment and implementation of an effective audit controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain appropriate and effective audit controls in full compliance with the requirements of HIPAA.
* Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all audit control-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Use hardware, software and/or procedural mechanisms that examine activity
* < List specific audit control procedures here >
* < List specific audit control procedures here >
* < List specific audit control procedures here >
* < List specific audit control procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
1. ***Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**

We proposed five technical security services requirements with supporting implementation features: Access control; **Audit controls**; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; **Audit trails**; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, **audit controls**, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

**Audit Controls (§ 164.312(b))**

We proposed that audit control mechanisms be put in place to record and examine system activity.

We adopt this requirement in this final rule.

**Access Control (§ 164.312(a)(1))**

*Comment*: We received a comment stating that "Audit controls" should be an implementation feature rather than the standard, and suggesting that we change the title of the standard to "Accountability," and provide additional detail to the audit control implementation feature.

*Response*: We do not adopt the term "Accountability" in this final rule because it is not descriptive of the requirement, which is to have the capability to record and examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security

*Comment*: One commenter recommended that this final rule state that audit control mechanisms should be implemented based on the findings of an entity's risk assessment and risk analysis. The commenter asserted that audit control mechanisms should be utilized only when appropriate and necessary and should not adversely affect system performance.

*Response*: We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care.

*Comment*: One commenter was concerned about the interplay of State and Federal requirements for auditing of privacy data and requested additional guidance on the interplay of privacy rights, laws, and the expectation for audits under the rule.

*Response*: In general, the security standards will supercede any contrary provision of State law. Security standards in this final rule establish a minimum level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to additional, or more stringent security measures. Section 1178(a)(2) of the statute provides several exceptions to this general rule. With regard to protected health information, the preemption of State laws and the relationship of the Privacy Rule to other Federal laws is discussed in the Privacy Rule beginning at 65 FR 82480; the preemption provisions of the rule are set out at 45 CFR part 160, subpart B.

It should be noted that although the Privacy Rule does not incorporate a requirement for an "audit trail" function, it does call for providing an accounting of certain disclosures of protected health information to an individual upon request. There has been a tendency to assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule's requirement for an audit capability will satisfy the Privacy Rule's requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**53: Data Integrity Controls Policy**

**Scope of Policy**

This policy governs Data Integrity Controls for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
* The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information (“PHI” and “ePHI”, as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
* The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
* Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Use encrypted methods of sending emails and files over a network.
* Use services such as HighTail and Voltage.
* < List specific data integrity control procedures here >
* < List specific data integrity control procedures here >
* < List specific data integrity control procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
1. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
	2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
2. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
	1. *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
	2. *Implementation specifications*:
		1. ***Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.**
		2. *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

**HHS Commentaries regarding Data Integrity Controls...**

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

*Transmission Security (§ 164.312(e)(1))*

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 54: Person or Entity Authentication Policy**

**Scope of Policy**

This policy governs Authentication of Persons or Entities seeking access to Electronic Protected Health Information in the possession of **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).
* The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information (“PHI” and “ePHI”, as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.
* The establishment and implementation of an effective Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
* Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
* Specific procedures shall be developed to specify the proper authentication of persons and entities who request access to individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA) on our computers, workstations and systems.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

**Procedures**

* Do not store save passwords on readily accessible ‘keychains’ on electronic devices.
* Use individual user ID names and passwords.
* < List specific person or entity authentication procedures here >
* < List specific person or entity authentication procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
1. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
	2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
2. ***Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**

**HHS Commentaries regarding Person or Entity Authentication...**

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

*Access Control (§ 164.312(a)(1))*

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity authentication" (see § 164.312(d)).

*Audit Controls (§ 164.312(b))*

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

*Integrity (§ 164.312(c)(1))*

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

*Person or Entity Authentication (§ 164.312(d))*

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone callback," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 55: Data Transmission Security Policy**

**Scope of Policy**

This policy governs Data Transmission Security for **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations pertaining to data transmission security, in accordance with the requirements at § 164.312(e)(1) and § 164.312(e)(2).
* The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
* The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information (“PHI”, as defined by HIPAA).

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to establish and implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
* Responsibility for the development and implementation of these Data Transmission Security Procedures shall reside with Name of Responsible Party or Person, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
* Specific Data Transmission Security Procedures shall be developed to protect individually identifiable health information, including Electronic Protected Health Information (“EPHI”, as defined by HIPAA).
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all Data Transmission Security Procedures, activities, and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

**Procedures**

* Use encrypted files, folders or devices to transmit ePHI
* Use services such as HighTail and Voltage that are encrypted.
* < List specific Data Transmission Security Procedures here >

**Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

|  |
| --- |
| **HHS Security Regulations as Amended January 2013Security Standards for the Protection of Electronic PHI: Technical Safeguards - § 164.312** |

A covered entity or business associate must, in accordance with § 164.306:

* 1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	2. *Implementation specifications*:
		1. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
		2. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		3. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		4. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
1. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
	2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
2. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
	1. *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
	2. *Implementation specifications*:
		1. *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		2. *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards

**Transmission Security (§ 164.312(e)(1))**

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

Last Revised: \_\_\_\_\_\_\_\_\_\_\_

**Policy 56: Mobile Device Policy**

**Scope of Policy**

This policy governs the use of mobile devices that can access, use, transmit, or store Individually Identifiable Health Information (“IIHI”), and Protected Health Information (“PHI”) in the custody of **PROVIDER COMPLIANCE SOLUTIONS**. All personnel of **PROVIDER COMPLIANCE SOLUTIONS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

**Assumptions**

* **PROVIDER COMPLIANCE SOLUTIONS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
* **PROVIDER COMPLIANCE SOLUTIONS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
* Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
* Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
* Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
* The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

**Policy Statement**

* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to extend all the privacy and security protections required by HIPAA to Protected Health Information accessed, used, transmitted, and stored on mobile devices operated by members of our workforce.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to include privacy and security issues related to mobile devices in our Risk Management process and analyses, to better understand risks inherent in the use of such devices.
* This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and are capable of receiving, processing, or transmitting Protected Health Information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Mobile Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile Devices include, but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).
* This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased by, and provided by **PROVIDER COMPLIANCE SOLUTIONS**.
* Mobile Devices which cannot be or have not been configured to comply with this Policy are prohibited.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to limit the access, use, transmittal, and storage of Protected Health Information exclusively to those mobile devices that can be configured and operated to deliver privacy and security comparable to the non-mobile data processing systems and devices that we operate.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to limit the access, use, transmittal and storage of Protected Health Information on mobile devices to the Minimum Necessary, as that term is defined in the HIPAA Regulations.
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit, or store Protected Health Information
* It is the Policy of **PROVIDER COMPLIANCE SOLUTIONS** to fully document all mobile device-related activities which involve Protected Health Information, in accordance with our Documentation Policy and the requirements of HIPAA.

**Procedures**

* No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by the IT Department/Security Office/etc Authorization will be given only for uses of Mobile Devices confirmed to have been configured to be compliant with this Policy.
* Any access, use, transmittal or storage of Protected Health Information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any **PROVIDER COMPLIANCE SOLUTIONS** facility or office, including an authorized home office or remote site, must be in compliance with all **PROVIDER COMPLIANCE SOLUTIONS** policies at all times.
* Authorization to use a Mobile Device may be suspended at any time:
	+ If the User fails or refuses to comply with this Policy;
	+ In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
	+ In connection with the investigation of a possible or proven security breach, security incident, or violation of **PROVIDER COMPLIANCE SOLUTIONS**’s policies;
	+ In order to protect life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of **PROVIDER COMPLIANCE SOLUTIONS**;
	+ Upon request of a supervisor or department head in which the User works; or
	+ Upon the direction of \_\_ insert Name of Position, Role, Department, or individual \_\_.
* Authorization to use a Mobile Device terminates:
	+ Automatically upon the termination of a User’s status as a member of **PROVIDER COMPLIANCE SOLUTIONS**’s workforce;
	+ Upon a change in the User’s role as a member of **PROVIDER COMPLIANCE SOLUTIONS**’s Workforce, unless continued authorization is authorized in writing.
	+ If it is determined that the User violated this or any other **PROVIDER COMPLIANCE SOLUTIONS** policy, in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction policy.
* The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
* At any time, any Mobile Device may be subject to audit to ensure compliance with this and other **PROVIDER COMPLIANCE SOLUTIONS** policies. Any User receiving such a request shall transfer possession of the Mobile Device to IT Department/Security Office/etc at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.
* < Add specific procedure here

**Compliance and Enforcement**

All **PROVIDER COMPLIANCE SOLUTIONS** managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER COMPLIANCE SOLUTIONS**’s Sanction Policy.

* ***Security Guidance for Remote Users* – Centers for Medicaid and Medicare Services**

 [www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf)

* ***An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* – National Institute of Standards and Technology (Publication No. SP800-66)**

...as well as other NIST I.T. Security papers and reports available from:

<http://csrc.nist.gov/publications/PubsSPs.html>