Answer

We have procedures in place to evaluate the effectiveness of our security policies and procedures, physical safeguards, and technical safeguards. Our evaluation is conducted periodically and in response to changes in the security environment.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(8) NIST CSF: ID.AM, ID.BE, ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.MI, RS.IM, RC.MI HICP: N/A	Required	Test	Fri Nov 25 12:12:43 MST 2022

Practice Information (1 location)

Practice Name	Arizona Physical Medicine & Rehabilitation
Address	20860 N. Tatum Blvd, Suite 300
City, State, Zip	Phoenix, AZ,
Phone, Fax	480-555-7885
Point of Contact	John Schmidt, DC
Title/Role	SRO
Phone	480-555-7885
Email	johnschmidtdc@dcseminars.com

Asset Information (2 total)

Risk	ID#	Type	Status	ePHI	Encryption	Assignment	Location
No		Laptop	Active [In-use and Assigned]	All of the above	Full disk encryption		
Yes		Desktop	Active [In-use and Assigned]	All of the above			

Business Associates and Vendors (2 total)

Vendor Name	Vendor Type	Satistfactory Assurances	Risk Assessed
		false	false
ABC Billing Company		true	true

Section 1, SRA Basics	Risk Score: 0 %
Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Has your practice completed a security risk assessment (SRA) before?

Answer	Yes.
Education	Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assesment.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 7, 10	Required	Test	Fri Nov 25 11:56:30 MST 2022

Q2. Do you review and update your SRA?

Answer	Yes.
Education	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:56:35 MST 2022

Q3. How often do you review and update your SRA?

Answer	Periodically and in response to operational changes and/or security incidents.
Education	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**

HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: N/A	Required	Test	Fri Nov 25 11:56:45 MST 2022

Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?

Answer
Yes.

Education
This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. A comprehensive security risk assessment should include all information systems that contain, process, or transmit ePHI. Maintain a complete and accurate inventory of the IT assets in your organization to facilitate the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: N/A NIST CSF: ID.RA, PR. DS, ID.AM HICP: TV1, Practice # 5	N/A	Test	Fri Nov 25 11:56:50 MST 2022

Q6. What do you include in your SRA documentation?

Answer
Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity. We develop corrective action plans as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe.

Education
This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. Establish a data classification policy that categorizes data as, for example, Sensitive, Internal Use, or Public Use. Identify the types of records relevant to each category. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or compromised data. IT asset management is critical to ensuring that the appropriate cyber hygiene controls are maintained across all assets in your organization, including medical device management.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 4, 5, 9	Required	Test	Fri Nov 25 11:56:59 MST 2022

Q7. Do you respond to the threats and vulnerabilities identified in your SRA?

Answer
Yes, we respond. We also maintain supporting documentation of our response.

Education

This is the most effective option.Threats and vulnerabilities should be documented within your SRA and given impact and likelihood ratings to determine severity. Safeguards protecting ePHI from these threats and vulnerabilities should be evaluated for effectiveness. Corrective action plans with plan of action milestones should be developed as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe. Risks should be formally deemed "accepted" only when appropriate. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, if patching is not automatic.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(B) NIST CSF: ID.RA, ID.RM, RS.MI HICP: TV1, Practice # 7	Required	Test	Fri Nov 25 11:57:05 MST 2022

Q8. Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Use internal or external experts to deploy security methodology.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(B) NIST CSF: ID.RA, ID.RM, RS.MI, ID.GV, PR.IP HICP: TV1, Practice # 7	Required	Test	Fri Nov 25 11:57:08 MST 2022

Q9. Do you communicate SRA results to personnel involved in responding to threats or vulnerabilities?

Answer

Yes.

Education

This is the most effective option. Communicate to workforce members who review and sign off after reading policies over a specified timeframe. The goal is to establish a standard practice for workforce members to review applicable policies and attest to the review, and for the organization to monitor compliance with this standard.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(B) NIST CSF: ID.RA, ID.RM, RS.MI, PR.IP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:57:21 MST 2022

Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?

Answer	Written and verbal communication as well as coordinated corrective action planning.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.Written results of the risk assessment should be communicated to the personnel responsible for responding to identified threats and vulnerabilities. The responsible persons should be involved in the creation of corrective action plans to mitigate threats and vulnerabilities for which they are responsible.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(B) NIST CSF: ID.RA, ID.RM, RS.MI HICP: N/A	Required	Test	Fri Nov 25 11:57:27 MST 2022

Section 2, Security Policies

Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?

Answer	Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.316(a) NIST CSF: ID.GV, ID.RA, PR.IP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:57:55 MST 2022

Q2. Do you review and update your security documentation, including policies and procedures?

Answer	Yes, we review and update our security documentation periodically and as necessary.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Review an appropriate number of policies over a specified timeframe. The goal is to establish a standard practice to review policies and to monitor compliance with this standard.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(iii) NIST CSF: ID.GV, ID.RA, PR.IP, RS.IM, RC.IM HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:57:58 MST 2022

Q3. How do you update your security program documentation, including policies and procedures?

Answer

We have a periodic review of information security policies that formally evaluates their effectiveness. Policies and procedures are updated as needed.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(iii) NIST CSF: ID.GV, ID.RA, PR.IP, RC.IM, RS.IM HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:00 MST 2022

Q4. Is the security officer involved in all security policy and procedure updates?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(iii) NIST CSF: ID.GV, ID.RA, PR.IP, RC.IM, RS.IM HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:05 MST 2022

Q5. How does documentation for your risk management and security procedures compare to your actual business practices?

Answer

Our risk management and security documentation completely and accurately reflects our actual business practices.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(1)(i) & (ii) NIST CSF: ID.BE, ID.RM, PR.IP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:10 MST 2022

Q6. How long are information security management and risk management documents kept?

Answer We maintain documents for at least six (6) years from the date of their creation or when they were last in effect, whichever is longer. These documents are maintained and backed up.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. The federal requirement is six (6) years retention of documentation, but your state or jurisdiction may have additional requirements.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(i) NIST CSF: ID.BE, ID.RM, PR.IP HICP: N/A	Required	Test	Fri Nov 25 11:58:19 MST 2022

Q7. Do you make sure that information security and risk management documentation is available to those who need it?

Answer Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(ii) NIST CSF: ID.BE, ID.RM, PR.IP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:22 MST 2022

Q8. How do you ensure that security and risk management documentation is available to those who need it?

Answer Appropriate workforce members receive instruction on our information security documentation and where to find it as part of their periodic privacy and security training. Documentation is securely made available to workforce members in physical or electronic formats.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Policies are established first and are then supplemented with procedures that enable the policies to be implemented. Policies describe what is expected, and procedures describe how the expectations are met.

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(ii) NIST CSF: ID.BE, ID.RM, PR.IP, ID.RA HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:24 MST 2022

Section 3, Security & Workforce

Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Who within your practice is responsible for developing and implementing information security policies and procedures?

Answer The security officer is a member of the workforce identified by name in policy documents.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO, PR.IP, ID.AM HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:40 MST 2022

Q2. Do you identify and document the role and responsibilities of the security officer?

Answer Yes. The security officer is identified by role and this is documented in our practice's information security policies, which describes the role's responsibilities.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO, PR.IP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 11:58:42 MST 2022

Q3. Is your security officer qualified for the position?

Answer

Yes. The security officer is an assigned member of the workforce familiar with security and has the ability to design, implement, and enforce security policies and procedures.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO HICP: N/A	Required	Test	Fri Nov 25 11:58:44 MST 2022

Q4. Do workforce members know who the security officer is?

Answer

Yes. Workforce members are aware of who our security officer is.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO HICP: N/A	Required	Test	Fri Nov 25 11:58:48 MST 2022

Q5. Do workforce members know how and when to contact the security officer?

Answer

Workforce members are made aware of the identity of the security officer and reasons for contacting the security officer as part of their orientation to the practice (upon hire) as well as periodic reminders of our internal policies and procedures (e.g. periodic review).

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO HICP: N/A	Required	Test	Fri Nov 25 11:58:50 MST 2022

Q7. How are roles and job duties defined as pertained to accessing ePHI?

Answer

We have written job descriptions, roles, and required qualifications documented for all workforce members with access to ePHI.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.Health care organizations of all sizes need to clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(A) NIST CSF: ID.AM, PR.MA, DE.CM, DE.DP, PR.IP HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 11:58:52 MST 2022

Q8. Do you screen your workforce members to verify trustworthiness?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(B) NIST CSF: DE.DP, PR.AC, PR.IP HICP: N/A	Addressable	Test	Fri Nov 25 11:58:54 MST 2022

Q9. How are your workforce members screened to verify trustworthiness?

Answer

Professional references are collected and verified. Criminal background checks are performed in addition to verifying licenses, credentials, and certifications .

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(3)(ii)(B) NIST CSF: DE.DP, PR.AC, PR.IP HICP: N/A	Addressable	Test	Fri Nov 25 11:58:56 MST 2022

Q10. Do you ensure that all workforce members (including management) are given security training?

Answer Yes, we ensure all workforce members complete security training on a periodic basis.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Establish and maintain a training program for your workforce that includes a section on phishing attacks. All users in your organization should be able to recognize phishing techniques. Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through e-mail. Train staff never to back up data on uncontrolled storage devices or personal cloud services. Train and regularly remind users that they must never share their passwords.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT , ID.RM, PR.IP HICP: TV1, Practice # 1, 4	Required	Test	Fri Nov 25 11:58:59 MST 2022

Q11. How do you ensure that all workforce members are given security training?

Answer We keep a list of workforce members who have completed security training. Trainings are provided upon hire and periodically thereafter. The list is reviewed and verified by the security officer.

Education This is an effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Train personnel to comply with organizational policies. At minimum, provide annual training on the most salient policy considerations, such as the use of encryption and PHI transmission restrictions. Provide staff with training on and awareness of phishing e-mails. Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT, PR.IP HICP: TV1, Practice # 1, 4, 10	Required	Test	Fri Nov 25 11:59:02 MST 2022

Q12. How long are records of workforce member security training kept?

Answer Records documenting the completion of required security trainings are kept for all workforce members (including management) and retained for at least six (6) years after completion of the training.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT, PR.IP HICP: N/A	Required	Test	Fri Nov 25 11:59:04 MST 2022

Q13. Are procedures in place for monitoring log-in attempts and reporting discrepancies?

Answer

Yes, these procedures workforce members' roles and responsibilities, log-in monitoring procedure, how to identify a log-in discrepancy and how to respond to an identified discrepancy.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement access management procedures to track and monitor user access to computers and programs.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(ii)(C) NIST CSF: DE.AE, DE.CM, RS.CO, PR.AT, PR.PT HICP: TV1, Practice # 3	Addressable	Test	Fri Nov 25 11:59:07 MST 2022

Q14. Is protection from malicious software (including timely antivirus/security updates and malware protection) covered in your procedures?

Answer

Yes. Software protection is included in our procedures. This includes a review of our procedures for guarding against malware, and the mechanisms in place for protection, and how procedures for workforce members to follow can to detect and report malicious software.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Antivirus (AV) software is readily available at low cost and is effective at protecting endpoints from computer viruses, malware, spam, and ransomware threats. Each endpoint in your organization should be equipped with antivirus software that is configured to update automatically. For medical devices, the medical device manufacturer should directly support AV software, or it should be cleared for operation by the manufacturer. Ensure that a compliant AV technology is enabled. If AV cannot be implemented, compensating controls should enforce an AV scan whenever the device is serviced prior to reconnecting to the device network.

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(5)(ii)(B) NIST CSF: PR.AT, PR.IP HICP: TV1, Practice # 2, 9	Addressable	Test	Fri Nov 25 11:59:10 MST 2022

Q15. What password security elements are covered in your security training?

Answer

Our security procedures include what our workforce roles/responsibilities are in password security, how to safeguard passwords, how to respond to a compromised password, and how to properly change a password using various password characteristics (e.g. many characters long, easy to remember, avoiding easy to guess phrases).

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. To stay current with best practices on security procedures consider enforcing password security measures consistent with guidance in NIST SP 800-63-3. Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access (e.g., Gmail, Yahoo, Facebook). For devices that are accessed off site, leverage technologies that use multi-factor authentication (MFA) before permitting users to access data or applications on the device. Logins that use only a username and password are often compromised through phishing e-mails. Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(5)(ii)(D) NIST CSF: PR.AT HICP: TV1, Practice # 2, 3	Addressable	Test	Fri Nov 25 11:59:15 MST 2022

Q16. Do you ensure workforce members maintain ongoing awareness of security requirements?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Establish and maintain a training program for your workforce that includes a section on phishing attacks. All users in your organization should be able to recognize phishing techniques. Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through e-mail. Train staff never to back up data on uncontrolled storage devices or personal cloud services.

References	**Compliance**	**Username**	**Audit Date**

HIPAA: §164.308(a)(5)(ii)(A) NIST CSF: PR.AT, ID.RA, ID.BE, ID.GV HICP: TV1, Practice # 1, 4	Addressable	Test	Fri Nov 25 11:59:19 MST 2022

Q17. How does your practice ensure workforce members maintain ongoing awareness of security requirements?

Answer	Formal trainings and periodic security reminders
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Provide staff with training on and awareness of phishing e-mails. Train personnel to comply with organizational policies. At minimum, provide annual training onthe most salient policy considerations, such as the use of encryption and PHI transmission restrictions.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(5)(ii)(A) NIST CSF: PR.AT, ID.RA, ID.BE, ID.GV HICP: TV1, Practice # 1, 4	Addressable	Test	Fri Nov 25 11:59:22 MST 2022

Q18. Do you have a sanction policy to enforce security procedures?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(C) NIST CSF: PR.IP HICP: N/A	Required	Test	Fri Nov 25 11:59:24 MST 2022

Q19. What is included in your sanction policy to hold personnel accountable if they do not follow your security policies and procedures?

Answer	All of the above.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(C) NIST CSF: PR.AT, RS.CO, PR.IP HICP: N/A	Required	Test	Fri Nov 25 12:01:37 MST 2022

Section 4, Security & Data	Risk Score: 0 %
Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Do you manage and control personnel access to ePHI, systems, and facilities?

Answer Yes.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. User accounts enable organizations to control and monitor each user's access to and activities on devices, EHRs, e-mail, and other third-party software systems. It is essential to protect user accounts to mitigate the risk of cyber threats.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.IP, PR.AC, PR.PT HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:00 MST 2022

Q2. How do you manage and control personnel access to ePHI, systems, and facilities?

Answer Detailed log of personnel and access levels based on role. Updates are reviewed by the security officer.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement single sign-on systems that automatically manage access to all software and tools once users have signed onto the network. Such systems allows the organization to centrally maintain and monitor access.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.IP, PR.AC, PR.PT HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:10 MST 2022

Q3. What is your process for authorizing, establishing, and modifying access to ePHI?

Answer Our security procedures designate personnel authorized to grant, review, modify, and terminate access. Access levels are reviewed and modified as needed.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Tailor access for each user based on the user's specific workplace requirements. Most users require access to common systems, such as e-mail and file servers. Implementing tailored access is usually called provisioning.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) NIST CSF: PR.AC, PR.IP HICP: TV1, Practice # 3	Addressable	Test	Fri Nov 25 12:00:12 MST 2022

Q4. How much access to ePHI is granted to users or other entities?

Answer Minimum access necessary based on the user's formal role.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the ##minimum necessary## principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and theft of data if the user's identity or access is compromised.

References	Compliance	Username	Audit Date
HIPAA: §164.502(b) NIST CSF: PR.AC, PR.IP, ID.RM, PR.DS HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:15 MST 2022

Q5. How are individual users identified when accessing ePHI ?

Answer Unique IDs and individual passwords are created for authorized workforce members and contractors in order access ePHI.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access (e.g., Gmail, Yahoo, Facebook).

References	Compliance	Username	Audit Date

HIPAA: §164.312(a)(2)(i) NIST CSF: PR.AC, PR.PT, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:17 MST 2022

Q6. Do you ensure all of your workforce members have appropriate access to ePHI?

Answer

Yes. We have written procedures to ensure workforce members' access privileges are minimum necessary (i.e. "need to know") based on their roles. These access privileges are approved by the security officer.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the ##minimum necessary## principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and theft of data if the user's identity or access is compromised.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.AC, PR.IP HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:19 MST 2022

Q7. How do you make sure that your workforce's designated access to ePHI is logical, consistent, and appropriate ?

Answer

Workforce members are granted access based on the minimum amount necessary for their role. This is consistently applied across the practice and any changes must be formally approved and documented.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Tailor access for each user based on the user's specific workplace requirements. Most users require access to common systems, such as e-mail and file servers. Implementing tailored access is usually called provisioning.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.PT, PR.IP, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:22 MST 2022

Q8. Do you use encryption to control access to ePHI?

Answer

Yes.

Education

This is the most effective option. Whenever reasonable and appropriate implement a mechanism to encrypt and decrypt ePHI. Install encryption software on every endpoint that connects to your EHR system, especially mobile devices such as laptops. Maintain audit trails of this encryption in case a device is ever lost or stolen. This simple and inexpensive precaution may prevent a complicated and expensive breach. If supported by the manufacturer, medical devices should have local encryption enabled in case the device is stolen. Implement an e-mail encryption module that enables users to securely send e-mails to externalrecipients or to protect information that should only be seen by authorized individuals.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(iv) NIST CSF: PR.DS, PR.MA, PR.PT HICP: TV1, Practice # 1, 4	Addressable	Test	Fri Nov 25 12:00:25 MST 2022

Q9. What procedures do you have in place to encrypt ePHI when deemed reasonable and appropriate?

Answer

Encryption is evaluated as part of our risk management process. We have procedures in place to encrypt data at rest (for example, USB drives or tapes) and in transit (for example, email or cloud EHR) whenever reasonable and appropriate, and find an alternative safeguard when not reasonable and appropriate.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Install encryption software on every endpoint that connects to your EHR system, especially mobile devices such as laptops. Maintain audit trails of this encryption in case a device is ever lost or stolen. This simple and inexpensive precaution may prevent a complicated and expensive breach. Provide regular training on encryption.

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(2)(ii) NIST CSF: PR.AC, PR.DS, PR.IP HICP: TV1, Practice # 1, 4	Addressable	Test	Fri Nov 25 12:00:28 MST 2022

Q10. Do you use alternative safeguards in place of encryption?

Answer

Yes. When encryption is not reasonable or appropriate, we implement an alternative safeguard.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. For devices that cannot be encrypted or that are managed by a third party, implement physical security controls to minimize theft or unauthorized removal. Examples include installation of anti-theft cables, locks on rooms where the devices are located, and the use of badge readers to monitor access to rooms where devices are located.

References	Compliance	Username	Audit Date

HIPAA: NIST CSF: ID.GV,PR.DS, PR.IP, ID.RA, PR.IP HICP: TV1, Practice # 2	Addressable	Test	Fri Nov 25 12:00:30 MST 2022

Q11. When encryption is deemed unreasonable or inappropriate to implement, do you document the use of an alternative safeguard?

Answer

Yes. We have policies and procedures to identify encryption capabilities of our devices and information systems. When encryption is not reasonable or appropriate, we implement an alternative safeguard and document it.

Education

Having policies and procedures to identify the encryption capabilities of your devices and information systems and then documenting when encryption is not reasonable or appropriate, and that you have implemented an alternative safeguard is the best practice. For devices that cannot be encrypted or that are managed by a third party, implement physical security controls to minimize theft or unauthorized removal. Examples include installation of anti-theft cables, locks on rooms where the devices are located, and the use of badge readers to monitor access to rooms where devices are located.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: NIST CSF: PR.DS HICP: TV1, Practice # 2	Addressable	Test	Fri Nov 25 12:00:33 MST 2022

Q12. Have you evaluated implementing any of the following encryption solutions in your local environment? (Full disk encryption, file/folder encryption, encryption of thumb drives or other external media)

Answer

All of the above.

Education

Encryption in these areas is critical to protecting ePHI in your local environment. Encryption applications prevent hackers from accessing sensitive data, usually by requiring a ##key## to encrypt and/or decrypt data. Prohibit the use of unencrypted storage, such as thumb drives, mobile phones, or computers. Require encryption of these mobile storage mediums before use.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(e)(2)(ii) NIST CSF: PR.AC, PR.DS, DE.CM, ID.RA, ID.RM HICP: TV1, Practice # 2	Addressable	Test	Fri Nov 25 12:00:36 MST 2022

Q13. Have you evaluated implementing encryption solutions for any of the following cloud services? (Email service, file storage, web applications, remote system backups)

Answer

All of the above.

Education Encryption in these areas is critical to protecting ePHI in your cloud environments. Contracts with EHR vendors should include language that requires medical/PHI data to be encrypted both at rest and during transmission between systems.

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(2)(ii) NIST CSF: HICP: TV1, Practice # 1	Addressable	Test	Fri Nov 25 12:00:39 MST 2022

Q14. Have you evaluated implementing any of the following encryption solutions for data in transit? (Encryption of internet traffic by means of a VPN, web traffic over HTTP encrypted email, or secure file transfer)

Answer All of the above.

Education Encryption in these areas is critical to protecting ePHI in transit. At minimum, provide annual training on the most salient policy considerations, such as the use of encryption and PHI transmission restrictions. Implement an e-mail encryption module that enables users to securely send e-mails to external recipients or to protect information that should only be seen by authorized individuals.

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(2)(ii) NIST CSF: HICP: TV1, Practice # 1, 4	Addressable	Test	Fri Nov 25 12:00:43 MST 2022

Q15. Do you periodically review your information systems for how security settings can be implemented to safeguard ePHI?

Answer Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, rendering it more difficult for hackers to maintain programs that are aligned with the most current version of that software application. Configure endpoints to patch automatically and ensure that third-party applications (e.g., Adobe Flash) are patched as soon as possible. Schedule and conduct vulnerability scans on servers and systems under your control toproactively identify technology flaws.Remediate flaws based on the severity of the identified vulnerability. This method is considered an ##unauthenticated scan.## The scanner has no extra sets of privileges to the server. It queries a server based on ports that are active and present for network connectivity. Each server isqueried for vulnerabilities based upon the level of sophistication of the software scanner.Conduct web application scanning of internet-facing webservers, such as web-based patientportals. Specialized vulnerability scanners can interrogate running web applications to identify vulnerabilities in the application design.Conduct routine patching of security flaws in servers, applications (including web applications),and third-party software. Maintain software at least monthly, implementing patches distributedby the vendor community, if patching is not automatic. Robust patch management processes mitigate vulnerabilities associated with obsolete software versions, whichare often easier for hackers to exploit.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(1) NIST CSF: PR.AC, PR.DS, ID.RA, PR.IP, DE.CM HICP: TV1, Practice # 2, 7	Required	Test	Fri Nov 25 12:00:45 MST 2022

Q16. How are you aware of the security settings for information systems which process, store, or transmit ePHI?

Answer

All systems which create, receive, maintain, or transmit ePHI (including any firewalls, databases, servers, and networked devices) have been examined to determine how security settings can be implemented to most appropriately protect ePHI.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Vulnerability scans may yield large amounts of data, which organizations urgently need to classify, evaluate, and prioritize to remediate security flaws before an attacker can exploit them.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(1) NIST CSF: PR.AC, PR.DS, PR.IP, ID.RA, PR.MA, PR.PT, DE.CM HICP: TV1, Practice # 7	Required	Test	Fri Nov 25 12:00:48 MST 2022

Q17. Do you use security settings and mechanisms to record and examine system activity?

Answer Yes.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. User accounts enable organizations to control and monitor each user's access to and activities on devices, EHRs, e-mail, and other third-party software systems.

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.DS, PR.PT, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:51 MST 2022

Q18. What mechanisms are in place to monitor or log system activity?

Answer Monitoring of system users, access attempts, and modifications. This includes a date/time stamp.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement access management procedures to track and monitor user access to computers and programs.

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.DS, PR.MA, PR.PT, DE.AE, DE.CM, RS.AN HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:54 MST 2022

Q19. How do you monitor or track ePHI system activity?

Answer System activity records are reviewed on a regular basis. The frequency of reviews is documented within our procedures. Results of activity reviews are also maintained, including activities which may prompt further investigation.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement access management procedures to track and monitor user access to computers and programs.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(D) NIST CSF: ID.RA, PR.DS, PR.MA, PR.PT, DE.AE, DE.CM, RS.AN HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:00:57 MST 2022

Q20. Do you have automatic logoff enabled on devices and platforms accessing ePHI?

Answer

Yes, automatic logoff is enabled on all devices and platforms to terminate access to ePHI after a set time of inactivity.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Configure systems and endpoints to automatically lock and log off users after a predetermined period of inactivity, such as 15 minutes.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(iii) NIST CSF: PR.AC, PR.DS HICP: TV1, Practice # 3	Addressable	Test	Fri Nov 25 12:01:00 MST 2022

Q21. Do you ensure users accessing ePHI are who they claim to be?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. The use of shared or generic accounts should be avoided. If shared accounts are required, train and regularly remind users that they must sign out upon completion of activity or whenever they leave the device, even for a moment. Passwords should be changed after each use. Sharing accounts exposes organizations to greater vulnerabilities. For example, the complexity of updating passwords for multiple users on a shared account may result in a compromised password remaining active and allowing unauthorized access over an extended period of time.

References	Compliance	Username	Audit Date
HIPAA: §164.312(d) NIST CSF: PR.AC, PR.DS, PR.MA, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:01:03 MST 2022

Q22. How do you ensure users accessing ePHI are who they claim to be?

Answer

Users authenticate themselves to access ePHI using the method authorized by our practice's policy and procedure (for example, user name and password, physical token, or biometric feature).

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Configure systems and endpoints to automatically lock and log off users after a predetermined period of inactivity, such as 15 minutes. Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

References	Compliance	Username	Audit Date
HIPAA: §164.312(d) NIST CSF: PR.AC, PR.DS, PR.MA, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:01:05 MST 2022

Q23. How do you determine the means by which ePHI is accessed?

Answer

All systems, devices, and applications which access ePHI are identified, evaluated, approved, and inventoried. Users can only access ePHI through these approved systems, devices, and applications.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access (e.g., Gmail, Yahoo, Facebook).

For devices that are accessed off site, leverage technologies that use multi-factor authentication (MFA) before permitting users to access data or applications on the device. Logins that use only a username and password are often compromised through phishing e-mails. Implement MFA authentication for the cloud-based systems that your organization uses to store or process sensitive data, such as EHRs. MFA mitigates the risk of access by unauthorized users.

References	Compliance	Username	Audit Date
HIPAA: §164.312(d) NIST CSF: PR.AC, PR.DS, PR.MA, DE.CM, PR.IP HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:01:08 MST 2022

Q24. Do you protect ePHI from unauthorized modification or destruction?

Answer

Yes. We have developed and implemented policies and procedures to protect ePHI from improper alteration or destruction.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lostor compromised data.

References	Compliance	Username	Audit Date
HIPAA: §164.312(c)(1) NIST CSF: PR.DS HICP: TV1, Practice # 4	Required	Test	Fri Nov 25 12:01:10 MST 2022

Q25. How do you confirm that ePHI has not been modified or destroyed without authorization?

Answer We have mechanisms (e.g. integrity verification tools) to corroborate that ePHI has not been altered or destroyed in an unauthorized manner or detect if such alteration occurs.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Establish a data classification policy that categorizes data as, for example, Sensitive, InternalUse, or Public Use. Identify the types of records relevant to each category. Implement data loss prevention technologies to mitigate the risk of unauthorized access to PHI.

References	Compliance	Username	Audit Date
HIPAA: §164.312(c)(2) NIST CSF: PR.DS, DE.CM, DE.AE HICP: TV1, Practice # 4	Addressable	Test	Fri Nov 25 12:01:12 MST 2022

Q26. Do you protect against unauthorized access to or modification of ePHI when it is being transmitted electronically?

Answer Yes. We have implemented technical security measures and procedures to prevent unauthorized access to and detect modification of transmitted ePHI.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. When e-mailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM),which is a nationally adopted secure e-mail protocol and network for transmitting PHI. DSM can be obtained from EHR vendors and other health information exchange systems. It was developed and adopted through the Meaningful Use program, and many medical organizations nationwide now use DSM networks. When texting PHI, use a secure texting system.

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(1) NIST CSF: PR.AC, PR.DS HICP: TV1, Practice # 1, 4	Required	Test	Fri Nov 25 12:01:14 MST 2022

Q27. Have you implemented mechanisms to record activity on information systems which create or use ePHI ?

Answer Yes. Activity on systems which create or use ePHI is recorded and examined. This is documented in our procedures, including a complete inventory of systems that record activity and how it is examined.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement single sign-on systems that automatically manage access to all software and tools once users have signed onto the network. Such systems allows the organization to centrally maintain and monitor access.

References	Compliance	Username	Audit Date

HIPAA: §164.312(b) NIST CSF: PR.AC, PR.DS, PR.PT, DE.AE, DE.CM, RS.AN, PR.MA HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:01:16 MST 2022

Section 5, Security and the Practice	Risk Score: 0 %
Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Do you manage access to and use of your facility or facilities [i.e. that house information systems and ePHI]?

Answer	Yes. We have written procedures in place restricting access to and use of our facilities.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AC, DE.CM, PR.IP HICP: TV1, Practice # 6	Required	Test	Fri Nov 25 12:01:49 MST 2022

Q2. What physical protections do you have in place to manage facility security risks?

Answer	We have methods for controlling and managing physical access to our facility such as, keypads, locks, security cameras, etc. We also have an inventory of our practice's facilities that house equipment that create, maintain, receive, and transmit ePHI.Our policies and procedures outline managements' involvement in facility access control and how authorization credentials for facility access are issued and removed for our workforce members and/or visitors. Workforce members' roles and responsibilities in facility access control procedures are documented and communicated.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks.Disable network ports that are not in use. Maintain network ports as inactive until an activation request is authorized. This minimizes the risk of an unauthorized user ##plugging in## to an empty port to access to your network.In conference rooms or waiting areas, establish guest networks that separate organizational data and systems. This separation will limit the accessibility of private data from guests visiting the organization. Validate that guest networks are configured to access authorized guest services only.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(ii) NIST CSF: ID.AM, PR.AC, PR.DS, DE.CM HICP: TV1, Practice # 6	Addressable	Test	Fri Nov 25 12:01:51 MST 2022

Q3. Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?

Answer

Yes. We have written policies and implemented procedures restricting access to equipment that house ePHI to authorized users only.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Restrict access to assets with potentially high impact in the event of compromise. This includes medical devices and internet of things (IoT) items (e.g., security cameras, badge readers, temperature sensors, building management systems).

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AC, DE.CM, PR.IP HICP: TV1, Practice # 6	Required	Test	Fri Nov 25 12:02:06 MST 2022

Q4. Do you manage workforce member, visitor, and third party access to electronic devices?

Answer

Yes. We have written procedures for classifying electronic devices, based on their capabilities, connection, and allowable activities; access to electronic devices by workforce members, visitors, and/or third parties is determined based on their classification.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. In conference rooms or waiting areas, establish guest networks that separate organizational data and systems. This separation will limit the accessibility of private data from guests visiting the organization. Validate that guest networks are configured to access authorized guest services only.

References	Compliance	Username	Audit Date

HIPAA: §164.310(b) NIST CSF: PR.AC, PR.DS, PR.PT, DE.CM, PR.IP HICP: TV1, Practice # 6	Required	Test	Fri Nov 25 12:02:09 MST 2022

Q5. Do you have physical protections in place, such as cable locks for portable laptops, screen filters for screen visible in high traffic areas, to manage electronic device security risks?

Answer

Yes. We have physical protections in place for all electronic devices and this is documented in policy and procedure.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Examples include installation of anti-theft cables, locks on rooms where the devices are located, and the use of badge readers to monitor access to rooms where devices are located.

References	Compliance	Username	Audit Date
HIPAA: §164.310(c) NIST CSF: PR.AC, PR.DS, PR.PT, DE.CM HICP: TV1, Practice # 6	Required	Test	Fri Nov 25 12:02:11 MST 2022

Q6. What physical protections do you have in place for electronic devices with access to ePHI?

Answer

We have robust procedures for electronic device access control such as, authorization for issuing new electronic device access and removing electronic device access. We also use screen filters, docking stations with locks, and/or cable locks for portable devices, privacy screens [walls or partitions], and/or secured proximity for servers and network equipment.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. For devices that cannot be encrypted or that are managed by a third party, implement physical security controls to minimize theft or unauthorized removal. Examples include installation of anti-theft cables, locks on rooms where the devices are located, and the use of badge readers to monitor access to rooms where devices are located. Disable network ports that are not in use. Maintain network ports as inactive until an activation request is authorized. This minimizes the risk of an unauthorized user ##plugging in## to an empty port to access to your network.

References	Compliance	Username	Audit Date
HIPAA: §164.310(c) NIST CSF: PR.AC, PR.DS, PR.PT, DE.CM HICP: TV1, Practice # 2, 6	Required	Test	Fri Nov 25 12:02:14 MST 2022

Q7. Do you keep an inventory and a location record of all of its electronic devices?

Answer

Yes. Our inventory list of all electronic devices and their functions is currently documented and updated on a periodic basis.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. A complete and accurate inventory of the IT assets in your organization facilitates the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet.

References	Compliance	Username	Audit Date
HIPAA: §164.310(b) NIST CSF: PR.AC, PR.DS, PR.PT, ID.AM HICP: TV1, Practice # 5	Required	Test	Fri Nov 25 12:02:16 MST 2022

Q8. Do you have an authorized user who approves access levels within information systems and locations that use ePHI?

Answer

Yes. We have written procedures outlining who has the authorization to approve access to information systems, location, and ePHI; how access requests are submitted; and how access is granted.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(A) NIST CSF: ID.AM, PR.MA, PR.PT, PR.IP HICP: TV1, Practice # 10	Addressable	Test	Fri Nov 25 12:02:21 MST 2022

Q9. Do you validate a person's access to facilities (including workforce members and visitors) based on their role or function?

Answer

Yes. We have procedures for validating access to our facility. Access levels are based on role or function. We also have strict requirements for validating workforce members or visitors who seek access to our critical systems and software programs.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.

References	Compliance	Username	Audit Date

HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AC, PR.DS, PR.PT, DE.CM, DE.CP, PR.IP HICP: TV1, Practice # 6	Addressable	Test	Fri Nov 25 12:02:23 MST 2022

Q10. How do you validate a person's access to your facility?

Answer

We maintain lists of authorized persons and have controls in place to identify persons attempting to access the practice, grant access to authorized persons, and prevent access by unauthorized persons.

Education

These are effective means of validating facility access. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AC, PR.DS, PR.PT, DE.CM, DE.CP HICP: TV1, Practice # 6	Addressable	Test	Fri Nov 25 12:02:26 MST 2022

Q11. Do you have access validation requirements for personnel and visitors seeking access to your critical systems (such as IT, software developers, or network admins)?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as you might restrict physical access to different parts of your medical office, it's important to restrict the access of third-party entities, including vendors, to separate networks. Allow them to connect only through tightly controlled interfaces. This limits the exposure to and impact of cyberattacks on both your organization and on the third-party entity.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AC, PR.DS, PR.PT, DE.CM, DE.CP, PR.IP HICP: TV1, Practice # 6	Addressable	Test	Fri Nov 25 12:02:28 MST 2022

Q12. Does this include controlling access to your software programs for testing and revisions?

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AC, PR.DS, PR.PT, DE.CM, DE.CP HICP: N/A	Addressable	Test	Fri Nov 25 12:02:30 MST 2022

Q13. Do you have procedures for validating a third party person's access to the facility based on their role or function?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as you might restrict physical access to different parts of your medical office, it's important to restrict the access of third-party entities, including vendors, to separate networks. Allow them to connect only through tightly controlled interfaces. This limits the exposure to and impact of cyberattacks on both your organization and on the third-party entity.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AC, PR.DS, PR.PT, DE.CM, DE.CP, PR.IP HICP: TV1, Practice # 6	Addressable	Test	Fri Nov 25 12:02:33 MST 2022

Q14. Do you have hardware, software, or other mechanisms that record and examine activity on information systems with access to ePHI?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement single sign-on systems that automatically manage access to all software and tools once users have signed onto the network. Such systems allows the organization to centrally maintain and monitor access.

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.AC, PR.DS, PR.PT, DE.AE, DE.CM, HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:02:35 MST 2022

Q15. What requirements are in place for retention of audit reports?

Answer	Our practice retains records of audit report review for a minimum of six (6) years, consistent with retention requirements for all information security documentation.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Your state or jurisdiction may have additional requirements beyond the six (6) year retention requirement.

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.DS, PR.PT, DE.AE, DE.CM, PR.IP HICP: N/A	Required	Test	Fri Nov 25 12:02:37 MST 2022

Q16. Do you maintain records of physical changes upgrades, and modifications to your facility?

Answer

Yes. We have written procedures to document modifications to our facility. This includes documenting when physical security component repairs, modifications, or updates are needed and our workforce members' roles and responsibilities in that process. Any changes to our facility's security components go through an authorization process.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(iv) NIST CSF: PR.DS, PR.MA HICP: N/A	Addressable	Test	Fri Nov 25 12:02:40 MST 2022

Q17. How do you maintain awareness of the movement of electronic devices and media?

Answer

We maintain a detailed inventory of all electronic devices and media which contain ePHI, including where they are located, which workforce members are authorized to access or possess the devices, and to where they are moved.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Although it can be difficult to implement and sustain IT asset management processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

References	Compliance	Username	Audit Date
HIPAA: §164.310(d)(2)(iii) NIST CSF: PR.MA, PR.PT, DE.AE, DE.CM, PR.DS HICP: TV1, Practice # 5, 10	Addressable	Test	Fri Nov 25 12:02:42 MST 2022

Q18. Are electronic devices secured?

Answer

Yes. We have procedures for safeguarding all electronic devices (such as screen guards, cable locks, locking storage rooms, cameras, and other physical features).

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. A small organization's endpoints must be protected. Endpoints include desktops, laptops, mobile devices, and other connected hardware devices (e.g., printers, medical equipment).

References	Compliance	Username	Audit Date
HIPAA: §164.310(c) NIST CSF: PR.AC, PR.DS, PR.PT, DE.CM HICP: TV1, Practice # 2	Required	Test	Fri Nov 25 12:02:45 MST 2022

Q19. Do you back up ePHI to ensure availability when devices are moved?

Answer

Yes. Our critical data and ePHI is centrally stored (such as in a cloud or active directory server) that can be accessed from any authorized device.

Education

This is an effective option to protect the confidentiality, integrity, and availability of ePHI. Make sure backups will be available and functional when needed through periodic testing. Train staff never to back up data on uncontrolled storage devices or personal cloud services. Leveraging the cloud for backup purposes is acceptable if you have established an agreement with the cloud vendor and verified the security of the vendor's systems.

References	Compliance	Username	Audit Date
HIPAA: §164.310(d)(2)(iv) NIST CSF: PR.DS, PR.IP HICP: TV1, Practice # 4	Addressable	Test	Fri Nov 25 12:02:47 MST 2022

Q20. Do you ensure devices which created, maintained, received, or transmitted ePHI are effectively sanitized when they are disposed of?

Answer

Yes. We remove any data storage or memory component from the device and then store it in a secure location. Data is wiped from the device prior to disposing of the device using a method that conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Although it can be difficult to implement and sustain IT asset management processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

References	Compliance	Username	Audit Date
HIPAA: §164.310(d)(1) NIST CSF: PR.AC, PR.DS, PR.PT, PR.IP HICP: TV1, Practice # 5	Required	Test	Fri Nov 25 12:02:50 MST 2022

Q21. How do you determine what is considered appropriate use of electronic devices and connected network devices?

Answer

We have documented policies and procedures in place outlining proper functions to be performed on electronic devices and devices (e.g. whether or not they should access ePHI), how those functions will be performed, who is authorized to use the devices, and the physical surroundings of the devices.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the ##minimum necessary## principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and theft of data if the user's identity or access is compromised.

References	Compliance	Username	Audit Date
HIPAA: §164.310(b) NIST CSF: PR.AC, PR.DS, PR.PT, DE.CM, ID.RA HICP: TV1, Practice # 4, 5	Required	Test	Fri Nov 25 12:02:53 MST 2022

Q22. Do you ensure access to ePHI is terminated when employment or other arrangements with the workforce member ends?

Answer

Yes. We have written procedures documenting termination or change of access to ePHI upon termination or change of employment, including recovery of access control devices (including organization-owned devices, media, and equipment), deactivation of information system access, appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI, time frames to terminate access to ePHI, and exit interviews that include a discussion of privacy and security topics regarding ePHI.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. When an employee leaves your organization, ensure that procedures are executed to terminate the employee's access immediately. Prompt user termination prevents former employees from accessing patient data and other sensitive information after they have left the organization. This is very important for organizations that use cloud-based systems where access is based on credentials, rather than physical presence at a particular computer. access based on the requirements for the new position. Similarly, if an employee changes jobs within the organization, it is important to terminate access related to the employee's former position before granting

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(C) NIST CSF: PR.AC, PR.IP HICP: TV1, Practice # 3	Addressable	Test	Fri Nov 25 12:02:56 MST 2022

Q23. Do you have procedures for terminating or changing third-party access when the contract, business associate agreement, or other arrangement with the third party ends or is changed?

Answer Yes

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. When an employee leaves your organization, ensure that procedures are executed to terminate the employee's access immediately. Prompt user termination prevents former employees from accessing patient data and other sensitive information after they have left the organization. This is very important for organizations that use cloud-based systems where access is based on credentials, rather than physical presence at a particular computer. access based on the requirements for the new position. Similarly, if an employee changes jobs within the organization, it is important to terminate access related to the employee's former position before granting

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(C) NIST CSF: PR.AC, PR.IP HICP: TV1, Practice # 3	Addressable	Test	Fri Nov 25 12:02:59 MST 2022

Q24. How do you ensure media is sanitized prior to re-use?

Answer

We have a process to completely purge data from all devices prior to re-use through device reimaging, degaussing, or other industry standard method; our method conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Education

This is an effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Ensure that obsolete data are removed or destroyed properly so they cannot be accessed by cyber-thieves. Just as paper medical and financial records must be fully destroyed by shredding or burning, digital data must be properly disposed of to ensure that they cannot be inappropriately recovered. Discuss options for properly disposing of outdated or unneeded data with your IT support. Do not assume that deleting or erasing files means that the data are destroyed.

References	Compliance	Username	Audit Date
HIPAA: §164.310(d)(2)(ii) NIST CSF: PR.IP, PR.MA HICP: TV1, Practice # 4	Required	Test	Fri Nov 25 12:03:01 MST 2022

Section 6, Security and Business Associates

Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Do you contract with business associates or other third-party vendors?

Answer Yes.

Education

Make sure all business associates and third-party vendors have been evaluated to determine whether or not they require a Business Associate Agreement.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: ID.GV HICP: N/A	Required	Test	Fri Nov 25 12:03:08 MST 2022

Q2. Do you allow third-party vendors to access your information systems and/or ePHI?

Answer Yes.

Education

Make sure all business associates and third-party vendors have been evaluated to determine whether or not they require a Business Associate Agreement. User accounts enable organizations to control and monitor each user's access to and activities on devices, EHRs, e-mail, and other third-party software systems. It is essential to protect user accounts to mitigate the risk of cyber threats.

References	Compliance	Username	Audit Date

HIPAA: N/A NIST CSF: ID.GV HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:03:11 MST 2022

Q3. How do you identify which business associates need access to create, receive, maintain, or transmit ePHI?

Answer

We review business associate contracts to determine which vendors or contractors require access to ePHI and we include a Business Associate Agreement (BAA) in our contract with them.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the ##minimum necessary## principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and theft of data if the user's identity or access is compromised.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AC, PR.DS HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:03:13 MST 2022

Q4. How does your practice enforce or monitor access for each of these business associates?

Answer

We determine degree of access based on the amount of ePHI accessed, the types of devices or mechanisms used for access, and our ability to control and monitor third-party access.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement access management procedures to track and monitor user access to computers and programs.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AC, PR.DS, DE.CM HICP: TV1, Practice # 3	Required	Test	Fri Nov 25 12:03:15 MST 2022

Q5. How do business associates communicate important changes in security practices, personnel, etc. to you?

Answer

Our BAAs include language describing how security-relevant changes should be communicated to our organization.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: ID.GV HICP: N/A	Required	Test	Fri Nov 25 12:03:18 MST 2022

Q6. Have you executed business associate agreements with all business associates who create, receive, maintain, or transmit ePHI on your behalf?

Answer Yes. We ensure all business associates have a fully executed BAA with us before creating, receiving, maintaining, or transmitting ePHI on our behalf.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(b)(3) NIST CSF: PR.AC HICP: N/A	Required	Test	Fri Nov 25 12:03:20 MST 2022

Q7. How do you maintain awareness of business associate security practices? (e.g. in addition to Business Associate Agreements)

Answer Our practice performs extra due diligence in the form of monitoring third-party connections to our information systems or other forms of access, in addition to including language for security compliance in our Business Associate Agreements (BAAs).

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: PR.AT, RS.CO, DE.CM HICP: N/A	Required	Test	Fri Nov 25 12:03:22 MST 2022

Q12. How does your practice document all of its business associates requiring access to ePHI?

Answer We maintain a current listing of all business associates with access to ePHI in addition to having Business Associate Agreements (BAAs) on file with any business associates with access to ePHI.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AC, PR.DS HICP: N/A	Required	Test	Fri Nov 25 12:03:24 MST 2022

Q13. Do you obtain Business Associate Agreements (BAAs) from business associates who access another covered entity's ePHI on your behalf?

Answer	Yes. We make sure to have BAAs in place with covered entities for which we are Business Associates as well as subcontractors to those covered entities who contract with us.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(2) NIST CSF: N/A HICP: N/A	Required	Test	Fri Nov 25 12:03:26 MST 2022

Section 7, Contingency Planning Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Section Questions

Q1. Does your practice have a contingency plan in the event of an emergency?

Answer	Yes.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP HICP: TV1, Practice # 8	Required	Test	Fri Nov 25 12:03:33 MST 2022

Q2. Is your contingency plan documented?

Answer	Yes.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**

HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP HICP: N/A	Required	Test	Fri Nov 25 12:03:35 MST 2022

Q3. Do you periodically update your contingency plan?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP, RS.IM, RC.IM HICP: N/A	Required	Test	Fri Nov 25 12:03:37 MST 2022

Q4. How do you ensure that your contingency plan is effective and updated appropriately?

Answer	We periodically review the plans contents, perform tests of the plan, and record the results. We revise the plan as needed and document this in policy.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(ii)(D) NIST CSF: RS.IM, ID.RA, PR.IP, RC.IM, ID.BE HICP: N/A	Required	Test	Fri Nov 25 12:03:40 MST 2022

Q5. Have you considered what kind of emergencies could damage critical information systems or prevent access to ePHI within your practice?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP, ID.RA HICP: N/A	Required	Test	Fri Nov 25 12:03:42 MST 2022

Q6. What types of emergencies have you considered?

Answer	All of the above.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP, ID.RA HICP: N/A	Required	Test	Fri Nov 25 12:24:34 MST 2022

Q7. Have you documented in your policies and procedures various emergency types and how you would respond to them?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP HICP: N/A	Required	Test	Fri Nov 25 12:03:47 MST 2022

Q8. Does your practice have policies and procedures in place to prevent, detect, and respond to security incidents?

Answer	Yes.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(6)(i) NIST CSF: DE.AE, RS.CO, RC.CO, PR.IP HICP: N/A	Required	Test	Fri Nov 25 12:03:49 MST 2022

Q9. How does your practice prevent, detect, and respond to security incidents?

Answer	All of the above.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(6)(i) NIST CSF: DE.AE, RS.CO, RC.CO, PR.IP, RS.IP HICP: TV1, Practice # 8	Required	Test	Fri Nov 25 12:24:38 MST 2022

Q10. Has your practice identified specific personnel as your incident response team?

Answer Yes.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Before an incident occurs, make sure you understand who will lead your incident investigation. Additionally, make sure you understand which personnel will support the leader during each phase of the investigation. At minimum, you should identify the top security expert who will provide direction to the supporting personnel.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(6)(ii) NIST CSF: RC.CO, ID.RM, PR.IP, DE.AE, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, ID.AM, ID.GV HICP: TV1, Practice # 8	Required	Test	Fri Nov 25 12:03:53 MST 2022

Q11. How are members of your incident response team identified and trained?

Answer Workforce members are trained on their role and responsibilities as part of the incident response team (upon hire) as well as periodic reminders of our internal policies and procedures and testing exercises.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. At minimum, you should identify the top security expert who will provide direction to the supporting personnel. Ensure that the leader is fully authorized to execute all tasks required to complete the investigation.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(6)(ii) NIST CSF: PR.AT, RC.CO, ID.RM, PR.IP, DE.AE, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, ID.AM, ID.RA HICP: TV1, Practice # 8	Required	Test	Fri Nov 25 12:03:55 MST 2022

Q12. Has your practice evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?

Answer

Yes, we have a process of evaluating all hardware and software systems, including those of business associates, to determine criticality of the systems and ePHI that would be accessed by executing our contingency plan. This is documented along with our asset inventory.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Define the standard practices for recovering IT assets in the case of a disaster, including backup plans.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP HICP: TV1, Practice # 10	Required	Test	Fri Nov 25 12:03:58 MST 2022

Q13. How would your practice maintain access to ePHI in the event of an emergency, system failure, or physical disaster?

Answer

We have established procedures and mechanisms for obtaining necessary electronic protected health information during an emergency.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(ii) NIST CSF: PR.AC, ID.BE, PR.DS, PR.IP, PR.MA, PR.PT, RS.RP, RS.CO HICP: N/A	Required	Test	Fri Nov 25 12:04:00 MST 2022

Q14. How would your practice maintain security of ePHI and crucial business processes before, during, and after an emergency?

Answer

We have robust contingency plans which provide for alternate site or other means for continued access to ePHI. We test them periodically to ensure continuity of security processes in an emergency setting.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(7)(ii)(C) NIST CSF: ID.BE, ID.RM, PR.IP, RS.RP, RS.CO, RS.AN, RC.CO, RC.RP HICP: N/A	Required	Test	Fri Nov 25 12:04:01 MST 2022

Q15. Do you have a plan for backing up and restoring critical data?

Answer	Yes, we have a plan for determining which data is critically needed, creating retrievable, exact copies of critical data and how to restore that data, including from alternate locations. We also test and revise the plan, as needed.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Define the standard practices for recovering IT assets in the case of a disaster, including backup plans.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(ii)(A),§164.308(a)(7)(ii)(B), and §164.308(a)(7)(ii)(E) NIST CSF: ID.BE, ID.RA, ID.RM, RS.AN, PR.IP, RS.RP, RS.CO, RC.CO, RC.RP, PR.DS HICP: TV1, Practice # 10	Required & Addressable	Test	Fri Nov 25 12:04:03 MST 2022

Q16. How is your practice's emergency procedure activated?

Answer	Upon identification or initiation of an emergency situation, emergency procedures are activated according to documented procedure, such as by formal communication from the security officer or other designated personnel.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(ii) NIST CSF: ID.BE, PR.IP, PR.PT, DE.DP, RS.RP, RS.CO HICP: N/A	Required	Test	Fri Nov 25 12:04:06 MST 2022

Q17. How is access to your facility coordinated in the event of disasters or emergency situations?

Answer We have written policies and procedures outlining facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency. Members of the workforce who need access to the facility in an emergency have been identified. Roles and responsibilities have been defined. A backup plan for accessing the facility and critical data is in place.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(i) NIST CSF: ID.BE, ID.RM, PR.AC, PR.IP, RS.RP, PR.DS, RS.CO, RC.RP HICP: N/A	Addressable	Test	Fri Nov 25 12:04:08 MST 2022

Q18. How is your emergency procedure terminated after the emergency circumstance is over?

Answer Upon the conclusion of the emergency situation, normal operations are resumed according to documented procedure, such as by formal communication from the security officer or other designated personnel.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(ii) NIST CSF: N/A HICP: N/A	Required	Test	Fri Nov 25 12:04:10 MST 2022

Q19. Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?

Answer Yes.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(8) NIST CSF: ID.AM, ID.BE, ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.MI, RS.IM, RC.MI HICP: N/A	Required	Test	Fri Nov 25 12:12:41 MST 2022

Q20. How do you evaluate the effectiveness of your security safeguards, including physical safeguards?