

# **RISK ANALYSIS & RISK MANAGEMENT PLAN**

## **7/11/2016**

Practice Name: Uptown Health Center

Address: 123 Anywhere

Anytown

NY

11785

Phone number:

Contact: John Doe



## **Users**

John Doe

## **Associates**

Name: Jill Doe

Type: Billing Company

Address: 200 Main Street, Smithtown, NY

Name: Global EHR

Type: EHR

Address: 123 Sparrow Rd, Miltown, WA

Name: Microsoft

Type: Email storage

Address:

## **Asset Inventory**

Asset ID: Computer HD

Description: Hard Drive

Has EPHI: Yes

Assignee: JD

Asset ID: Copier

Description: Copier

Has EPHI: Yes

Assignee: JD



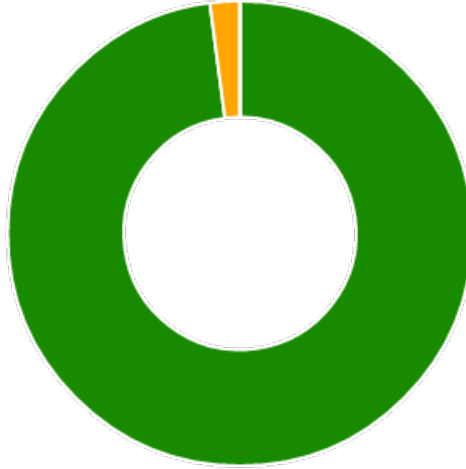
Administrative



Physical



Technical



Combined



Table View

ID ▲	Citation ◆	Answer ◆	Flagged ◆	Risk Level ◆	Current Activities ◆	Notes ◆	Remediation ◆	Reason ◆	Last Edit ◆
A01	§164.308(a)(1)(i)	Yes		Low	We have office PNP's			N/A	[JD]7/11/2016 12:06:04 am
A02	§164.308(a)(1)(i)	Yes		Low	We perform an SRA on a periodic basis and make updates accordingly.			N/A	[JD]6/28/2016 3:45:10 pm
A04	§164.308(a)(1)(ii)(A)	Yes		Low	An SRA is performed when there are significant organizational changes.			N/A	[JD]7/1/2016 9:34:12 pm
A05	§164.308(a)(1)(ii)(B)	Yes		Low	Part our PNP's.			N/A	[JD]7/11/2016 12:08:20 am
A07	§164.308(a)(1)(ii)(B)	Yes		Low	We perform am SRA and distribute to appropriate staff members.			N/A	[JD]6/28/2016 3:52:49 pm
A08	§164.308(a)(1)(ii)(B)	Yes			This is done as part of our SRA.			N/A	[JD]6/28/2016 3:53:10 pm
A14	§164.308(a)(2)	Yes	✓	Medium	Part of the team includes IT personnel qualified to IS security.			N/A	[JD]7/11/2016 12:10:48 am
A57	§164.308(a)(8)	Yes		Low	We perform assessments when there are operational changes or enviromental factors.			N/A	[JD]7/11/2016 12:15:37 am
A58	§164.308(a)(8)	Yes		Low	We monitor safeguards			N/A	[JD]7/11/2016 12:16:56 am
A59	§164.308(a)(8)	Yes			We have a SRO			N/A	[JD]6/28/2016 3:56:28 pm
PH10	§164.310(a)(2)(ii)	Yes		Low	As part of our office PNP's. We use back up systems in the event of an emergency.	JD: Battery and cloud back up.		N/A	[JD]7/11/2016 12:26:40 am
PO01	§164.316(a)	Yes		Low	The PNP's are updated as necessary.			N/A	[JD]6/28/2016 3:57:12 pm
PO02	§164.316(b)(1)(i)	Yes			Office PNP's are written and available in paper and electronic form			N/A	[JD]7/11/2016 12:18:44 am
PO03	§164.316(b)(1)(ii)	Yes		Low	We keep related regulation and policies in electronic form			N/A	[JD]7/11/2016 12:19:52 am
PO04	§164.316(b)(2)(i)	Yes		Low	We retain documents for 6 years			N/A	[JD]6/29/2016 10:29:34 am
PO05	§164.316(b)(2)(ii)	Yes			We use role based access controls			N/A	[JD]7/11/2016 12:21:51 am
PO06	§164.316(b)(2)(iii)	Yes			We update or PNP periodically and as needed.			N/A	[JD]7/11/2016 12:24:08 am

ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities ♦	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A03	§164.308(a)(1)(ii)(A)	Yes		Low	We perform a SRA as required to identify possible vulnerabilities.			N/A	[JD]7/11/2016 12:35:34 am
A20	§164.308(a)(3)(i)	Yes	✓	Low	As part of our office PNP's we use the least privilege access			N/A	[JD]7/11/2016 12:43:22 am
A21	§164.308(a)(3)(i)	Yes		Low	The SRO			N/A	[JD]6/28/2016 4:08:49 pm
A23	§164.308(a)(3)(ii)(A)	Yes		Low	Duties are segregated so that no one person has too much access and control to threaten patient security.			N/A	[JD]7/11/2016 12:44:29 am
A24	§164.308(a)(3)(ii)(A)	Yes		Low	Employees sign confidentiality agreements.			N/A	[JD]7/11/2016 12:46:18 am
A25	§164.308(a)(3)(ii)(A)	No		Low	Non workforce members do not have access			Practice Size	[JD]6/28/2016 4:10:32 pm
A26	§164.308(a)(3)(ii)(B)	Yes		Low	Employees sign confidentiality agreements			N/A	[JD]7/11/2016 12:48:09 am
A28	§164.308(a)(3)(ii)(C)	Yes		Low	SRO terminates authorization as part of our office PNP's			N/A	[JD]6/28/2016 4:11:34 pm
A29	§164.308(a)(3)(ii)(C)	Yes		Low	As part of our office PNP's			N/A	[JD]6/28/2016 4:12:16 pm
PH11	§164.310(a)(2)(ii)	Yes		Low	As part of our office PNP's. We have a security plan for natural, environmental and human threats.			N/A	[JD]7/11/2016 12:28:23 am
PH19	§164.310(b)	Yes		Low	We have a log of all devices			N/A	[JD]7/11/2016 12:36:13 am
PH20	§164.310(b)	Yes		Low	We have developed and implemented PNP's for work station policies.			N/A	[JD]7/11/2016 12:29:41 am
PH25	§164.310(c)	Yes		Low	As part of our office PNP's we use PW, encrypted backup and email.	JD: We use encrypted devices with cloud based IS		N/A	[JD]7/11/2016 12:42:35 am
T25	§164.312(b)	Yes		Low	Most of not all questions are categorized.			N/A	[JD]7/11/2016 12:31:45 am
T37	§164.312(d)	Yes		Low	We utilize documented UN and PWs, use RBAC and encrypted servers and email.	JD: This needs to be performed when on boarding and exiting		N/A	[JD]7/11/2016 12:33:56 am

ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities ♦	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A30	§164.308(a)(4)(i)	Yes		Low	We employ the principles of least privilege and min nec access			N/A	[JD]7/11/2016 12:50:53 am
A31	§164.308(a)(4)(ii)(B)	Yes		Low	As part of our office PNP's			N/A	[JD]7/11/2016 12:52:03 am
A32	§164.308(a)(4)(ii)(C)	Yes		Low	Duites are segregated	JD: SRO needs to update		N/A	[JD]7/11/2016 12:53:00 am
A33	§164.308(a)(4)(ii)(C)	Yes			As part of our office PNP's we assign UN and PW and change them as necessary			N/A	[JD]7/11/2016 12:53:30 am
PH13	§164.310(a)(2)(iii)	Yes			As part of our office PNP's. SRO ensures that all UN are updated and hardware is accounted			N/A	[JD]7/11/2016 12:54:46 am
PH14	§164.310(a)(2)(iii)	Yes		Low	We use limited access			N/A	[JD]7/11/2016 12:57:24 am
PH21	§164.310(b)	Yes		Low	As part of our office PNP's. We use minimal access controls.			N/A	[JD]7/11/2016 12:58:31 am
PH22	§164.310(c)	Yes		Low	We utilize auto log off after one minute of non-use.			N/A	[JD]7/11/2016 12:59:15 am
PH29	§164.310(c)	Yes		Low	PNP states that all devices must be PW protected and only access information from encrypted cloude servers and email			N/A	[JD]7/11/2016 1:00:51 am
T01	§164.312 (a)(1)	Yes		Low	SRO assigns levels of authorization based on RBAC			N/A	[JD]7/11/2016 1:01:30 am
T02	§164.312 (a)(1)	Yes		Low	As part of our office PNP's based on RBAC			N/A	[JD]7/11/2016 1:03:28 am
T03	§164.312 (a)(1)	Yes		Low	SRO and owner determine RBAC			N/A	[JD]7/11/2016 1:03:54 am
T04	§164.312 (a)(1)	Yes		Low	SRO assigns UN and PW. We use encrypted servers and email.			N/A	[JD]7/11/2016 1:05:14 am
T05	§164.312(a)(2)(i)	Yes		Low	SRO assigns user ID			N/A	[JD]7/11/2016 1:05:34 am
T06	§164.312(a)(2)(i)	Yes		Low	Every user must use their own UN and PW			N/A	[JD]7/11/2016 1:07:06 am
T17	§164.312 (a)(2)(iii)	Yes		Low	After 1 minute			N/A	[JD]6/28/2016 4:22:22 pm



ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities ♦	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A06	§164.308(a)(1)(ii)(B)	Yes		Low	As part of our office PNP's and staff training.			N/A	[JD]7/11/2016 1:15:08 am
T18	§164.312 (a)(2)(iii)	Yes		Low	Users are trained on proper log off procedures			N/A	[JD]7/11/2016 1:08:01 am
T19	§164.312 (a)(2)(iii)	Yes		Low	After 5 minutes			N/A	[JD]7/11/2016 1:08:16 am
T20	§164.312 (a)(2)(iv)	Yes		Low	We use encrypted servers and email			N/A	[JD]7/11/2016 10:24:58 am
T21	§164.312 (a)(2)(iv)	Yes		Low	We use high level encrypted devices			N/A	[JD]7/11/2016 10:25:24 am
T22	§164.312 (a)(2)(iv)	Yes		Low	We use encrypted harddrives and certified cloud based EHR.			N/A	[JD]6/29/2016 10:48:35 am
T32	§164.312(c)(1)	Yes	✓	Low	W monitor access on the backend of EHR			N/A	[JD]7/11/2016 10:26:21 am
T33	§164.312(c)(2)	Yes		Low	EHR leaves a digital footprint			N/A	[JD]7/11/2016 10:27:16 am
T34	§164.312(d)	Yes	✓	Low	The SRO performs verification of all persons when onboarding.	JD: This is probably difficult to enforce therefore we need staff help.	Consider use of a biometric device.	N/A	[JD]7/11/2016 1:11:40 am
T35	§164.312(d)	Yes	✓	Low	We use one email account for the office.	JD: Contact IT person		N/A	[JD]7/11/2016 1:12:58 am
T36	§164.312(d)	Yes	✓	Low	We currently use UN and PW. Consider biometrics.			N/A	[JD]7/11/2016 1:14:22 am
T38	§164.312(e)(1)	Yes		Low	We use encrypted email			N/A	[JD]7/11/2016 10:27:45 am
T39	§164.312(e)(1)	Yes		Low	We use encrypted email and call intended recipients.			N/A	[JD]7/11/2016 10:28:17 am
T40	§164.312(e)(2)(i)	Yes	✓	Low	We use encrypted email and cloud storage			N/A	[JD]7/11/2016 10:30:56 am
T41	§164.312(e)(2)(i)	Yes		Low	WE use encrypted servers and email			N/A	[JD]7/11/2016 10:31:30 am

ID ▲	Citation ◆	Answer ◆	Flagged ◆	Risk Level ◆	Current Activities ◆	Notes ◆	Remediation ◆	Reason ◆	Last Edit ◆
PH01	§164.310(a)(1)	Yes		Low	We keep an inventory of all devices, systems and media. We limit access to these areas.			N/A	[JD]7/11/2016 10:50:39 am
PH02	§164.310(a)(1)	Yes		Low	We keep all systems in an environmentally safe room			N/A	[JD]7/11/2016 10:52:44 am
PH03	§164.310(a)(1)	Yes		Low	We review access PNPs			N/A	[JD]7/11/2016 10:53:51 am
PH04	§164.310(a)(1)	Yes		Low	We have a security camera in the entrance and lock all doors and windows.			N/A	[JD]7/11/2016 10:57:19 am
PH08	§164.310(a)(2)(ii)	Yes		Low	We inventory keys, doors, locks and we change combination on a routine basis			N/A	[JD]7/11/2016 10:59:55 am
PH09	§164.310(a)(2)(ii)	Yes		Low	We rekey locks if a key is lost and change alarm codes when someone terminates employment.			N/A	[JD]7/11/2016 11:01:55 am
PH30	§164.310(d)(1)	Yes	✓	Low	Our devices are locked in secure location.			N/A	[JD]7/11/2016 10:35:06 am
PH31	§164.310(d)(1)	Yes		Low	These are removed and destroyed			N/A	[JD]7/11/2016 10:35:28 am
PH32	§164.310(d)(1)	Yes		Low	We keep records of all devices and who owns them			N/A	[JD]7/11/2016 10:36:10 am
PH33	§164.310(d)(1)	Yes	✓	Low	We wipe devices clean or destroy them			N/A	[JD]7/11/2016 10:38:06 am
PH34	§164.310(d)(2)(i)	Yes	✓	Low	We wipe the device of any information			N/A	[JD]7/11/2016 10:38:40 am
PH35	§164.310(d)(2)(ii)	Yes		Low	We wipe all information off devices and use cloud storage			N/A	[JD]7/11/2016 10:39:31 am
PH38	§164.310(d)(2)(iv)	Yes		Low	Data is backed up to an encrypted server			N/A	[JD]7/11/2016 10:39:51 am
T10	§164.312(a)(2)(ii)	Yes		Low	We save information to an encrypted cloud based storage that we have a BAA agreement with them			N/A	[JD]7/11/2016 10:49:51 am
T42	§164.312(e)(2)(i)	Yes		Low	We use the encrypted email servers and have a BAA with them.			N/A	[JD]7/11/2016 10:32:09 am
T43	§164.312(e)(2)(ii)	Yes		Low	We use the encrypted servers and have a BAA with them.			N/A	[JD]7/11/2016 10:32:32 am
T44	§164.312(e)(2)(ii)	Yes		Low	We use encrypted servers			N/A	[JD]7/11/2016 10:34:21 am

ID ▲	Citation ◆	Answer ◆	Flagged ◆	Risk Level ◆	Current Activities ◆	Notes ◆	Remediation ◆	Reason ◆	Last Edit ◆
A09	§164.308(a)(1)(ii)(C)	Yes		Low	Part of our office PNP's enforcement			N/A	[JD]7/11/2016 11:58:23 am
A10	§164.308(a)(1)(ii)(C)	Yes		Low	PNPs include a sanction policy			N/A	[JD]7/11/2016 11:59:55 am
A13	§164.308(a)(2)	Yes		Low	We have a SRO			N/A	[JD]7/11/2016 12:00:07 pm
A15	§164.308(a)(2)	Yes			The SRO has job duties			N/A	[JD]7/11/2016 12:01:37 pm
A16	§164.308(a)(2)	Yes		Low	Staff are trained and know who the SRO is in the office			N/A	[JD]7/11/2016 12:03:44 pm
A17	§164.308(a)(3)(i)	Yes		Low	We keep a list of workforce members, separate duties and implement minimum use requirements.			N/A	[JD]7/11/2016 12:08:23 pm
A19	§164.308(a)(3)(i)	Yes		Low	We employ least priveledge access and controls			N/A	[JD]7/11/2016 12:10:08 pm
PH12	§164.310(a)(2)(iii)	Yes		Low	We have a facility access list			N/A	[JD]7/11/2016 11:07:30 am
PH16	§164.310(a)(2)(iii)	Yes		Low	We have a security camera in the entrance of the office and PIN codes on the lock where PHI is stored. W also do background checks on all employees.			N/A	[JD]7/11/2016 11:48:46 am
PH18	§164.310(a)(2)(iv)	Yes		Low	We document repairs and modifications			N/A	[JD]7/11/2016 11:49:17 am
PH23	§164.310(c)	Yes		Low	Screens are shielded from secondary viewers		Turn monitors away from third party viewers	N/A	[JD]7/11/2016 11:54:16 am
PH24	§164.310(c)	No		Medium	We do not have public devices			Practice Size	[JD]7/11/2016 11:54:55 am
PH26	§164.310(c)	Yes	✓		Locks on all devices			N/A	[JD]7/11/2016 11:55:26 am
PH27	§164.310(c)	Yes		Low	We perform periodic reviews to ensure privacy		video cameras to monitor work stations	N/A	[JD]7/11/2016 11:56:13 am
PH28	§164.310(c)	Yes		Low	locked doors, screen protection, video survelance.			N/A	[JD]7/11/2016 11:57:54 am

ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities ♦	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A16	§164.308(a)(2)	Yes		Low	Staff are trained and know who the SRO is in the office			N/A	[JD]7/11/2016 12:12:04 pm
A18	§164.308(a)(3)(i)	Yes		Low	We monitor BA activity			N/A	[JD]7/11/2016 12:43:19 pm
A22	§164.308(a)(3)(ii)(A)	Yes		Low	All employees have written job descriptions that include HIPAA responsibilities			N/A	[JD]7/11/2016 12:11:12 pm
A27	§164.308(a)(3)(ii)(B)	Yes		Low	Background checks and credit reports yearly			N/A	[JD]7/11/2016 12:11:27 pm
A34	§164.308(a)(5)(i)	Yes		Low	Staff are trained continuously			N/A	[JD]7/11/2016 12:13:14 pm
A35	§164.308(a)(5)(i)	Yes		Low	Training is updated			N/A	[JD]7/11/2016 12:15:11 pm
A36	§164.308(a)(5)(i)	Yes		Low	We provide training for all workforce members			N/A	[JD]7/11/2016 12:17:06 pm
A37	§164.308(a)(5)(i)	Yes		Low	The workforce members are trained on a continual basis.			N/A	[JD]7/11/2016 12:20:07 pm
A38	§164.308(a)(5)(i)	Yes		Low	We keep training records			N/A	[JD]7/11/2016 12:25:07 pm
A39	§164.308(a)(5)(ii)(A)	Yes		Low	We conduct periodic meetings and have postings on updated security matters			N/A	[JD]7/11/2016 12:28:08 pm
A40	§164.308(a)(5)(ii)(B)	Yes		Low	Staff are trained about updating anti-virus, malware, etc.			N/A	[JD]7/11/2016 12:29:27 pm
A41	§164.308(a)(5)(ii)(B)	Yes		Low	Staff are trained and advised not to open unknown emails.			N/A	[JD]7/11/2016 12:32:47 pm
A42	§164.308(a)(5)(ii)(C)	Yes		Low	Workforce is trained about phishing, malware and malicious attacks.			N/A	[JD]7/11/2016 12:35:39 pm
A43	§164.308(a)(5)(ii)(D)	Yes		Low	Each staff member has their own UN and PW for devices and security system			N/A	[JD]7/11/2016 12:42:02 pm
A60	§164.308(b)(1)	Yes	✓		SRO monitors all BAA			N/A	[JD]7/11/2016 12:45:21 pm
A61	§164.308(b)(1)	Yes		Low	We maintain an updated list of all BA and their access to PHI	JD: Be sure to monitor this		N/A	[JD]7/11/2016 12:48:03 pm
A62	§164.308(b)(1)	Yes			We obtain BAA from BA			N/A	[JD]7/11/2016 12:48:27 pm

ID ▲	Citation ◆	Answer ◆	Flagged ◆	Risk Level ◆	Current Activities ◆	Notes ◆	Remediation ◆	Reason ◆	Last Edit ◆
A49	§164.308(a)(7)(i)	Yes		Low	We use cloud based EHR			N/A	[JD]7/11/2016 1:33:59 pm
A50	§164.308(a)(7)(i)	Yes		Low	We use cloud based EHR and email servers			N/A	[JD]7/11/2016 1:34:37 pm
A51	§164.308(a)(7)(i)	Yes		Low	We review and revise the COOP as necessary			N/A	[JD]7/11/2016 1:35:29 pm
A52	§164.308(a)(7)(ii)(A)	Yes		Low	We use cloud based back up and/or EHR			N/A	[JD]7/11/2016 1:36:04 pm
A53	§164.308(a)(7)(ii)(B)	Yes		Low	We use cloud based EHR and email			N/A	[JD]7/11/2016 1:36:34 pm
A54	§164.308(a)(7)(ii)(C)	Yes		Low	We use encrypted cloud based EHR and email			N/A	[JD]7/11/2016 1:38:15 pm
A55	§164.308(a)(7)(ii)(D)	Yes		Low	We test each year			N/A	[JD]7/11/2016 1:38:27 pm
A56	§164.308(a)(7)(ii)(E)	Yes		Low	We use encrypted cloud based EHR			N/A	[JD]7/11/2016 1:39:31 pm
A63	§164.308(b)(2)	Yes		Low	We acquire BAA from them and get assurances that they are HIPAA compliant.			N/A	[JD]7/11/2016 12:59:05 pm
A64	§164.308(b)(3)	Yes		Low	We obtain a BAA from all contractors who have access to PHI			N/A	[JD]7/11/2016 1:00:01 pm
O1	§164.314(a)(1)(i)	Yes		Low	We obtain assurances that the BA safeguards ePHI			N/A	[JD]7/11/2016 1:00:38 pm
O2	§164.314(a)(2)(i)	Yes		Low	We use the HHS OCR BAA			N/A	[JD]7/11/2016 1:01:29 pm
O3	§164.314(a)(2)(iii)	Yes		Low	We ensure that all downstream BA implement safeguards through the BAA			N/A	[JD]7/11/2016 1:12:54 pm
PH05	§164.310(a)(2)(i)	Yes		Low	We use certified EHR			N/A	[JD]7/11/2016 1:46:27 pm
PH06	§164.310(a)(2)(i)	Yes		Low	We use cloud based backup and email			N/A	[JD]7/11/2016 1:49:18 pm
PH07	§164.310(a)(2)(i)	Yes		Low	We use cloud based EHR and data file storage			N/A	[JD]7/11/2016 1:51:55 pm
T07	§164.312(a)(2)(ii)	Yes		Low	WE have a written contingency plan			N/A	[JD]7/11/2016 1:52:55 pm

ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A11	§164.308(a)(1)(ii)(D)	Yes		Low	The SRO reviews access of EHR and emails			N/A	[JD]7/11/2016 2:06:27 pm
A12	§164.308(a)(1)(ii)(D)	Yes		Low	The SRO monitors activity			N/A	[JD]7/11/2016 2:06:54 pm
PH15	§164.310(a)(2)(iii)	Yes	✓	Medium	We keep a log of visitors who have access to PHI		Implement a policy for this	N/A	[JD]7/11/2016 2:08:21 pm
PH17	§164.310(a)(2)(iv)	Yes		Low	We maintain a written record of physical changes			N/A	[JD]7/11/2016 2:09:08 pm
PH36	§164.310(d)(2)(iii)	Yes		Low	The SRO records movement of HW and SW. Most of what we use is cloud based so there is less of a threat.			N/A	[JD]7/11/2016 2:10:10 pm
PH37	§164.310(d)(2)(iii)	Yes		Low	We record when data is taken off site. Again, since we use cloud based EHR and email that is encrypted this is less of a concern.			N/A	[JD]7/11/2016 2:15:11 pm
T08	§164.312(a)(2)(ii)	Yes		Low	These are identified in our PNPs			N/A	[JD]7/11/2016 1:58:38 pm
T09	§164.312(a)(2)(ii)	Yes		Low	We use cloud based storage and email			N/A	[JD]7/11/2016 1:59:04 pm
T11	§164.312(a)(2)(ii)	Yes		Low	We use offsite backup of EHR			N/A	[JD]7/11/2016 1:59:26 pm
T12	§164.312(a)(2)(ii)	Yes		Low	We use cloud based EHR			N/A	[JD]7/11/2016 2:00:04 pm
T13	§164.312(a)(2)(ii)	Yes		Low	The SRO activates these procedures			N/A	[JD]7/11/2016 2:02:10 pm
T14	§164.312(a)(2)(ii)	Yes		Low	The SRO is responsible			N/A	[JD]7/11/2016 2:02:31 pm
T15	§164.312(a)(2)(ii)	Yes		Low	We test access to our EHR and cloud based files			N/A	[JD]7/11/2016 2:04:04 pm
T16	§164.312(a)(2)(ii)	Yes		Low	We use cloud based EHR			N/A	[JD]7/11/2016 2:05:07 pm
T23	§164.312(b)	Yes		Low	We use cloud based EHR which leaves a digital footprint and email that sends a copy of all emails to the SRO			N/A	[JD]7/11/2016 2:16:50 pm
T24	§164.312(b)	Yes		Low	Our cloud based EHR tracks usage. This is tracked periodically.			N/A	[JD]7/11/2016 2:19:16 pm

ID ▲	Citation ♦	Answer ♦	Flagged ♦	Risk Level ♦	Current Activities ♦	Notes ♦	Remediation ♦	Reason ♦	Last Edit ♦
A44	§164.308(a)(6)(i)	Yes		Low	We have enforcement policies in place			N/A	[JD]7/11/2016 2:23:48 pm
A45	§164.308(a)(6)(ii)	Yes		Low	The SRO responds to all incidents			N/A	[JD]7/11/2016 2:25:23 pm
A46	§164.308(a)(6)(ii)	Yes		Low	The SRO is in charge of training staff			N/A	[JD]7/11/2016 2:28:07 pm
A47	§164.308(a)(6)(ii)	Yes		Low	We have PNP			N/A	[JD]7/11/2016 2:33:55 pm
A48	§164.308(a)(6)(ii)	Yes		Low	We use _____ software			N/A	[JD]7/11/2016 2:34:23 pm
T26	§164.312(b)	Yes		Low	We perform a SRA when necessary			N/A	[JD]7/11/2016 2:19:38 pm
T27	§164.312(b)	Yes		Low	We use cloud based EHR that leaves a digital footprint and we use email that sends a copy of all emails to the SRO			N/A	[JD]7/11/2016 2:20:32 pm
T28	§164.312(b)	Yes		Low	The SRA is distributed to all relevant individuals			N/A	[JD]7/11/2016 2:21:20 pm
T29	§164.312(b)	Yes		Low	The audit reports are reviewed by the SRO			N/A	[JD]7/11/2016 2:21:42 pm
T30	§164.312(b)	Yes		Low	We keep files for 6 years or longer per OCR requirements			N/A	[JD]7/11/2016 2:22:16 pm
T31	§164.312(b)	Yes	✓	Low	Records are kept by the SRO	JD: Check with EHR company about access reports		N/A	[JD]7/11/2016 2:23:05 pm