Security Risk Assessment Tool

Application Version: 3.5.1

Detailed Report

TechNova

04-06-2025

DISCLAIMER
The Security Risk Assessment Tool at http://HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights (OCR) Health Information Privacy website at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool. Updated: August 18, 2023

Section 1, SRA Basics		Risk Score: 100 %
Threats & Vulnerabilities		Risk Rating
Inadequate risk awareness or failure to identify new weaknesses		
	Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches	Critical
	Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)	Medium
	Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or destruction from animals/insects	Low
	Man-made threat(s) such as insider carelessness, theft/vandalism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals	Low
	Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions	Low
Failure to remediate known risk(s)		
	Information disclosure (ePHI, proprietary, intellectual, or confidential)	Critical
	Penalties from contractual non-compliance with third-party vendors	Medium
	Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems	Medium
	Data deletion or corruption of records	Medium
	Prolonged exposure to hacker, computer criminal, malicious code, or careless insider	Low
	Corrective enforcement from regulatory agencies (e.g., HHS, OCR, FTC, CMS, State or Local jurisdictions)	Medium
	Hardware/equipment malfunction	Medium
Failure to meet minimum regulatory requirements and security standards		
	Corrective enforcement from regulatory agencies (e.g., HHS, OCR, FTC, CMS, State or Local jurisdictions)	Critical
	Damage to public reputation due to breach	Critical

	Failure to attain incentives or optimize value-based reimbursement	Medium
	Litigation from breach victims due to lack of reasonable and appropriate safeguards	Critical
Inadequate Asset Tracking		
	Information disclosure (ePHI, proprietary, intellectual, or confidential)	Critical
	Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems	Critical
	Unauthorized use of assets or changes to data within information systems	Medium
	Unauthorized installation of software or applications	Critical
	Loss, theft, or disruption of assets	Medium
	Improper operation/configuration of assets	Medium
Unspecified workforce security responsibilities		
	Non-remediated weaknesses	Medium
	Prolonged duration of addressing non-remediated weaknesses	Medium
	Insider carelessness exposing ePHI or causing disruption to information systems and business processes	Medium

Section Questions

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

Answer	No.
Education	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, GV.OC, PR.DS, PR.PS, RS.MI HPH CPG: 1 HICP: TV1 - Practice # 7, 10	Required	James Del Ciello	Sun Apr 06 11:55:02 PDT 2025

Q5. How do you ensure you are meeting current HIPAA security regulations?

Answer	I don't know.
Education	An accurate and thorough security risk assessment should be performed, reviewed and updated periodically, or in response to operational changes, security incidents, or the occurrence of a significant event.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(B) NIST CSF: GV.RR, GV.PO, GV.OV, GV.RM HPH CPG: 1 HICP: TV1 - Practice # 10	Required	James Del Ciello	Sun Apr 06 11:55:18 PDT 2025

Section 2, Security Policies	Risk Score: 100 %
Threats & Vulnerabilities	Risk Rating
Failure to update Policies & Procedures	
Fines/penalties from mandated regulatory requirements	Critical
Unstructured guidance for daily tasks and duties within workforce	Medium
Failure to share security procedure information with appropriate parties	
Unauthorized access to ePHI or sensitive information permitted	Critical
Disruption of information system function	Critical
ePHI accessed by unauthorized entities	Critical
Insider carelessness causing disruption	Critical
Insider carelessness exposing ePHI	Critical
Inconsistent/unclear risk management documentation	
Unclear security coordination across workforce	Medium
Unstructured guidance for daily tasks and duties	Medium
No risk management documentation (or low retention of documentation)	
Fines/penalties from regulatory enforcement	Critical

	Inability of workforce to perform proper security and privacy-related tasks or access procedural documents	Critical
	Unstructured workforce coordination of risk management procedures	Medium

Section Questions

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

Answer	No, we do not maintain documentation on our information security activities or risk management.
Education	You should document policies and procedures to ensure you consistently make informed decisions on the effective monitoring, identification, and mitigation of risks to 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: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS HPH CPG: 1, 14, 15 HICP: TV1 - Practice # 10	Required	James Del Ciello	Sun Apr 06 12:01:42 PDT 2025

Section 3, Security & Workforce Risk Score: 100 %

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 not formally named or otherwise identified in policy.
Education	You should have a qualified and capable person appointed to the responsibility of security officer. Having a central point of contact helps ensure that information security practices are coordinated, consistent, and that the organization can be held accountable. 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.AE, GV.RR, RS.CO, PR.PS, ID.AM HPH CPG: 4 HICP: TV1 - Practice # 10	Required	James Del Ciello	Sun Apr 06 12:04:07 PDT 2025

Q6. Who do people contact for security considerations if there is NO security officer?

Answer	Other.
Education	In order to meet the standard, you should identify a member of your workforce to serve as the security official and who will be responsible for the development and implementation of security policies and procedures. If you do not have a designated security officer, your workforce may not be able to execute immediate and appropriate mitigating actions when there are security problems.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO HPH CPG: 4 HICP: N/A	N/A	James Del Ciello	Sun Apr 06 12:04:30 PDT 2025

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

Answer	We do not have written job roles or responsibilities for workforce members with access to ePHI.
Education	Consider implementing procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. If such procedures are determined to not be reasonable and appropriate, document the reason why and what is being done to compensate for these lack of procedures. 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.AE, PR.PS HPH CPG: 6, 7 HICP: TV1 - Practice #2, 3	Required	James Del Ciello	Sun Apr 06 12:04:56 PDT 2025

Q8. Do you screen your workforce members (e.g., staff, volunteers, interns) with tools like credential verification or background checks to verify trustworthiness?

Answer	I don't know.
Education	Unqualified or untrustworthy users could access your ePHI if policies and procedures do not require screening workforce members prior to enabling access to facilities, information systems, and ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(B) NIST CSF: DE.AE, PR.AA, PR.IR, PR.PS HPH CPG: 6 HICP: N/A	Addressable	James Del Ciello	Sun Apr 06 12:05:07 PDT 2025

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

Answer	I don't know.
Education	Provide periodic security trainings to all workforce members. The standard states that periodic security trainings be completed and documented for all workforce members, and the documentation is reviewed by your practice's security officer. 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 , GV.RM, PR.PS HPH CPG: 4 HICP: TV1 - Practice # 1, 4	Required	James Del Ciello	Sun Apr 06 12:05:24 PDT 2025

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

Answer	Log-in monitoring tools are available but we do not actively utilize them.
Education	Consider revising your procedures to include roles and responsibilities, how to identify a log-in discrepancy, and how to respond to an identified discrepancy. If doing so is determined to not be reasonable and appropriate, document the reason why and what compensating control takes its place. 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.PS HPH CPG: 18 HICP: TV1 - Practice #2, 3	Addressable	James Del Ciello	Sun Apr 06 12:05:33 PDT 2025

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

Answer	Yes. Our security procedures include a review of our practice's procedure for guarding against malicious software, but does not cover how workforce members can detect and report malicious software or the protection mechanisms and system capabilities in place for malware protection.
Education	Consider including software protection in your procedures, such as: 1. What protection mechanisms and system capabilities are in place for protection against malicious software, 2. Workforce members' roles and responsibilities in malicious software protection procedures, 3. Steps to protect against and detect malicious software, and 4. Actions on how to respond to malicious software infections. 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.PS HPH CPG: 1, 2 HICP: TV1 - Practice # 2, 9	Addressable	James Del Ciello	Sun Apr 06 12:05:52 PDT 2025

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

Answer	Our security procedures include some but not all of the items noted above.
Education	Consider enforcing password security measures consistent with guidance in NIST SP 800-63-3 as part of your security training. If this is not determined to be reasonable and appropriate, document the reason why along with your compensating control. 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 HPH CPG: 2, 8 HICP: TV1 - Practice # 2, 3	Addressable	James Del Ciello	Sun Apr 06 12:06:28 PDT 2025

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

Answer	I don't know.
Education	Consider securing your workforce with formal, regular trainings as well as periodic reminders. If these steps are not determined to be reasonable and appropriate, document the reason why along with your compensating control. 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, GV.OC, GV.RR, GV.PO, GV.OV HPH CPG: 4 HICP: TV1 - Practice # 1, 4	Addressable	James Del Ciello	Sun Apr 06 12:06:36 PDT 2025

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

Answer	I don't know.
Education	Consider looking into whether your practice has a sanction policy. It is required that your practice be able to apply appropriate sanctions against workforce members who fail to comply with your practice's security policies and procedures.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(C) NIST CSF: PR.PS HPH CPG: N/A HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:06:46 PDT 2025

Section 4, Security & Data Risk Score: 70 %

Threats & Vulnerabilities	Risk Rating

Section Questions

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

Answer	No.

Education	Consider implementing policies and procedures to determine, authorize, and control access of workforce members to ePHI, systems, and facilities as appropriate. 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.PS, PR.AA, PR.IR HPH CPG: 6 HICP: TV1 - Practice #2, 3	Required	James Del Ciello	Sun Apr 06 12:07:49 PDT 2025

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

Answer	Access levels are granted, modified, and terminated as needed, but we do not have formal procedures.
Education	You should implement a formal security procedure and designate authorized personnel to grant, review, modify, and terminate access. Access levels should be reviewed and modified as needed. 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.AA, PR.IR, PR.PS HPH CPG: 6 HICP: TV1 - Practice # 3	Addressable	James Del Ciello	Sun Apr 06 12:08:00 PDT 2025

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

Answer	I don't know.
Education	Policies and procedures outlining how users are granted only the minimum necessary access to ePHI should be documented and implemented based on the user role. Allowing a high degree of access to ePHI may have negative impacts to your practice. Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your 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.AA, PR.IR, PR.PS, GV.RM, PR.DS HPH CPG: 3, 9 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:08:07 PDT 2025

Q5. How are individual users identified when accessing ePHI?

Answer	Generic usernames and/or shared passwords are used in order to access ePHI.
Education	If you do not have policies requiring use of a unique identifier for all users accessing ePHI, you might not be able to keep track of authorized users and the roles and responsibilities assigned to them. 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.AA, PR.IR, DE.CM HPH CPG: 8, 9 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:08:33 PDT 2025

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

Answer	Yes. We verbally communicate access privileges to our workforce members but we do not have written procedures.
Education	You should implement and document procedures to ensure workforce members have access privileges based on their role and no higher than necessary to perform their duties. These procedures and access privileges should be appropriately approved and communicated. 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.AA, PR.IR, PR.PS HPH CPG: 9 HICP: TV1 - Practice # 3,4	Required	James Del Ciello	Sun Apr 06 12:09:04 PDT 2025

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

Answer	We do not have a procedure for ensuring user access is appropriate for their role.
Education	Review role-based access to determine how specific you can designate access for users, based on their roles. Implement and document procedures to ensure minimum necessary access is in place across the board to the extent reasonable and appropriate. If access exceptions are commonly granted, they should be documented and policies should be in place outlining the procedure for access exceptions. 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.PS, DE.CMHPH CPG: 3, 8, 9 HICP: TV1 - Practice # 3,4	Required	James Del Ciello	Sun Apr 06 12:09:21 PDT 2025

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

Answer	I don't know.
Education	You might not be able to ensure access to ePHI is denied to unauthorized users if you do not use encryption/decryption methods to control access to ePHI and other health information. 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 external recipients 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 HPH CPG: 5 HICP: TV1 - Practice # 1, 4	Addressable	James Del Ciello	Sun Apr 06 12:09:26 PDT 2025

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: N/A NIST CSF: GV.RR, GV.PO, GV.OV, PR.DS, PR.PS, ID.RA HPH CPG: 5 HICP: TV1 - Practice # 2	Addressable	James Del Ciello	Sun Apr 06 12:09:46 PDT 2025

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

Answer	I don't know.
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: N/A NIST CSF: PR.DS HPH CPG: 5 HICP: TV1 - Practice # 2	Addressable	James Del Ciello	Sun Apr 06 12:09:57 PDT 2025

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	I don't know.
Education	Consider reviewing and evaluating all the locations where you are processing, storing, or transmitting ePHI and whether it is reasonable to implement encryption. Encryption can help safeguard your ePHI, whether you are transmitting it over the Internet, backing it up on a server, or just carrying a mobile device or your laptop to and from your facility. Encrypting ePHI makes it completely unreadable to anyone but you or its intend recipient. 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.AA, PR.IR, PR.DS, DE.CM, ID.RA, GV.RM HPH CPG: 5 HICP: TV1 - Practice # 2	Addressable	James Del Ciello	Sun Apr 06 12:10:09 PDT 2025

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

Answer	Some of the above.
Education	Consider reviewing and evaluating all the locations where you are processing, storing, or transmitting ePHI and whether it is reasonable to implement encryption. Encryption can help safeguard your ePHI, whether you are transmitting it over the Internet, backing it up on a server, or just carrying a mobile device or your laptop to and from your facility. Encrypting ePHI makes it completely unreadable to anyone but you or its intended recipient. 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: N/A HPH CPG: 5 HICP: TV1 - Practice # 1	Addressable	James Del Ciello	Sun Apr 06 12:10:26 PDT 2025

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	I don't know
Education	Consider reviewing and evaluating all the locations where you are processing, storing, or transmitting ePHI and whether it is reasonable to implement encryption. Encryption can help safeguard your ePHI, whether you are transmitting it over the Internet, backing it up on a server, or just carrying a mobile device or your laptop to and from your facility. Encrypting ePHI makes it completely unreadable to anyone but you or its intended recipient. At minimum, provide annual training on the most important 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: N/A HPH CPG: 5 HICP: TV1 - Practice # 1, 4	Addressable	James Del Ciello	Sun Apr 06 12:10:35 PDT 2025

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

Answer	No.
Education	Consider periodically reviewing the security settings on all systems which process, store, or transmit ePHI for how you can implement mechanisms to protect 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 to proactively 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 is queried for vulnerabilities based upon the level of sophistication of the software scanner. Conduct web application scanning of internet-facing webservers, such as web-based patient portals. 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 distributed by the vendor community, if patching is not automatic. Robust patch management processes mitigate vulnerabilities associated with obsolete software versions, which are often easier for hackers to exploit.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(1) NIST CSF: PR.AA, PR.IR, PR.DS, ID.RA, PR.PS, DE.CM HPH CPG: 1, 16, 18, 20 HICP: TV1 - Practice # 2, 7	Required	James Del Ciello	Sun Apr 06 12:10:42 PDT 2025

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

Answer	We are aware that systems have security settings to protect ePHI but have not reviewed all systems comprehensively.
Education	Consider reviewing security settings for all systems which process, store, and transmit 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.AA, PR.IR, PR.DS, PR.PS, ID.RA, PR.MA, DE.CM HPH CPG: 1, 18, 20 HICP: TV1 - Practice # 7	Required	James Del Ciello	Sun Apr 06 12:10:58 PDT 2025

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

Answer	I don't know.
Education	Consider looking into whether your practice has implemented hardware, software, and/or procedural mechanisms to monitor system activity. To meet the requirement, your practice should have system monitoring mechanisms in place where ePHI is accessible. 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, DE.CM HPH CPG: 14, 15, 16, 18, 20 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:11:05 PDT 2025

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, DE.AE, DE.CM, RS.AN HPH CPG: 14, 15, 16, 18, 20 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:11:28 PDT 2025

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

Answer	System activity records are reviewed as needed but not on a regular basis. Results of activity reviews are maintained, including activities which may prompt further investigation.

Education	Ensure your practice is able to detect and prevent security incidents by regularly reviewing system activity information as part of its ongoing operations and following security incidents. 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, DE.AE, DE.CM, RS.AN HPH CPG: 14, 15, 16, 18, 20 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:11:43 PDT 2025

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

Answer	Automatic time-out is enabled on electronic devices accessing ePHI, but automatic logoff to fully terminate the session is not enabled.
Education	Consider implementing automatic logoff on all devices and platforms which access ePHI. If this is not determined to be reasonable and appropriate, document the reason why and what compensating control is in its place. 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.AA, PR.IR, PR.DS HPH CPG: 11 HICP: TV1 - Practice # 3	Addressable	James Del Ciello	Sun Apr 06 12:11:58 PDT 2025

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

Answer	I don't know.
Education	Procedures should be in place to verify users accessing ePHI are who they claim to be, such as user authentication. 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.AA, PR.IR, PR.DS, PR.MA, DE.CM HPH CPG: 3, 8 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:12:08 PDT 2025

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

Answer	Applications which access ePHI are identified, evaluated, approved, and inventoried, but we do not manage which devices can access these applications (e.g., workforce members' personal devices accessing a cloud-based EHR without first identifying and approving the device)
Education	Unsecured points could compromise data accessed through an otherwise secure application. Consider implementing a device management process to ensure security standards are in place for all points accessing 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.AA, PR.IR, PR.DS, PR.MA, DE.CM, PR.PS HPH CPG: 3, 8 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:12:40 PDT 2025

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

Answer	Yes. We have some procedures to protect the integrity of our ePHI but these may not be totally comprehensive.
Education	Implement policies and procedures to protect ePHI from unauthorized modification or destruction, such as user activity monitoring or data validation tools. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or compromised data.

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

HIPAA: §164.312(c)(1) NIST CSF: PR.DS HPH CPG: N/A HICP: TV1 - Practice # 4	Required	James Del Ciello	Sun Apr 06 12:12:53 PDT 2025

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

Answer	We manually monitor changes made to ePHI in systems with audit log functionality, but do not have automated systems.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. You may want to consider implementing automated electronic mechanisms and/or integrity verification tools. 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. 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 HPH CPG: 16, 17, 18 HICP: TV1 - Practice # 4	Addressable	James Del Ciello	Sun Apr 06 12:13:06 PDT 2025

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.AA, PR.IR, PR.DS HPH CPG: 17 HICP: TV1 - Practice # 1, 4	Required	James Del Ciello	Sun Apr 06 12:13:34 PDT 2025

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.AA, PR.IR, PR.DS, PR.PS, DE.AE, DE.CM, RS.AN, PR.MA HPH CPG: 18 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:13:48 PDT 2025

Q28. Does the organization stay up to date or informed (e.g., cybersecurity listserv monitoring) on emerging threats and vulnerabilities that may affect information systems?

Answer	Yes, the organization subscribes to cybersecurity listservs and other informational sources that supply information regarding legal and regulatory requirements pertaining to cybersecurity emerging threats.
Education	This is the most effective option of those provided to track and manage current legal and regulatory requirements on protection of individuals information and understanding emerging cybersecurity threats. Subscribing to notifications from IT authoritative sources on threats and vulnerabilities such as CISA, ISO/IEC, H-ISAC, or IT-ISAC is a starting point for keeping abreast of the most current information available.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.OC HPH CPG: 14, 15 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:14:04 PDT 2025

Q29. Is there a process in place to identify and evaluate information systems for potential emerging technical vulnerabilities and how the exposure could affect systems that contain ePHI?

Answer	Yes, periodic vulnerability scans or penetration testing are done on a regular, scheduled basis to assess network computing and physical and system architecture for weaknesses, and software systems that may have reached their end of life.

Education	This is the most effective option among those provided to identify potential new threats and vulnerabilities within the information system. Timely information about technical vulnerabilities should be evaluated to identify the organizations exposure to vulnerabilities and appropriate measures should be taken to address the risk. The organization should identify any patch or software configuration and software end of life that needs to be addressed as well as assess all facilities that house critical computing assets for physical vulnerabilities and resilience issues. The organization should monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services and review processes and procedures for weaknesses that could be exploited to affect cybersecurity.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.OC HPH CPG: 1 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:14:23 PDT 2025

Q30. If new threats or vulnerabilities are identified through regular scanning, what is done to mitigate and respond to them?

Answer	The organization applies their policy and procedures consistent with the risk assessment to mitigate identified vulnerabilities.
Education	This is the most effective option among those provided to respond to and mitigate identified risks. The organization applies the policy and procedures consistent with the risk assessment to mitigate any identified vulnerabilities in a risk appropriate way. In addition, the organization tracks the progress of risk response implementation and uses findings to inform risk response decisions and actions.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.OC HPH CPG: 16 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:14:38 PDT 2025

Section 5, Security and the Practice

Risk Score: 60 %

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.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7 HICP: TV1 - Practice # 6	Required	James Del Ciello	Sun Apr 06 12:15:06 PDT 2025

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

Answer	We have written procedures documenting how authorization credentials for facility access are issued and removed for our workforce members and/or visitors.
Education	Ensure only authorized access to ePHI and facilities is allowed by implementing policies and procedures to limit physical access systems and facilities housing ePHI. Consider implementing policies and procedures to safeguard the facility and equipment from unauthorized tampering, theft, or physical access. 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.AA, PR.IR, PR.DS, DE.CM HPH CPG: 7, 16 HICP: TV1 - Practice # 6	Addressable	James Del Ciello	Sun Apr 06 12:15:46 PDT 2025

Q3. Do you restrict physical access to and use of your equipment (i.e., equipment that house ePHI)?

Answer	No. We do not have a process to restrict access to equipment that house ePHI to authorized users.
Education	Ensure only authorized access to ePHI is allowed by implementing and documenting procedures to govern access to equipment that house 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.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7, 11 HICP: TV1 - Practice # 6	Required	James Del Ciello	Sun Apr 06 12:17:05 PDT 2025

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

Answer	No. We do not have a process for managing workforce member, visitor, or third-party access to electronic devices.
Education	With regard to workstation-use and physical security, implement policies and procedures that define how electronic devices are used to access 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.AA, PR.IR, PR.DS, DE.CM, PR.PS HPH CPG: 10, 6 HICP: TV1 - Practice #4, 6	Required	James Del Ciello	Sun Apr 06 12:17:14 PDT 2025

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 some physical protections in place for some, but not all, electronic devices.
Education	Implement physical safeguards for all electronic devices that access electronic protected health information, to restrict access to authorized users. Examples include installation of anti-theft cables, locks on rooms where the devices are located, screen protectors or dividers, 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.AA, PR.IR, PR.DS, DE.CM HPH CPG: 11 HICP: TV1 - Practice # 6	Required	James Del Ciello	Sun Apr 06 12:17:32 PDT 2025

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

Answer	We have limited procedures for electronic device access control including some but not all of those listed above.
Education	Consider which physical safeguards to protect access to ePHI can be reasonably and appropriately implemented in your practice. Consider an authorization process for issuing new electronic device access and removing electronic device access. Or using 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. 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.AA, PR.IR, PR.DS, DE.CM HPH CPG: 11 HICP: TV1 - Practice # 2, 6	Required	James Del Ciello	Sun Apr 06 12:17:47 PDT 2025

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.AA, PR.IR, PR.DS, ID.AM HPH CPG: 11 HICP: TV1 - Practice # 5	Required	James Del Ciello	Sun Apr 06 12:17:58 PDT 2025

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 in place describing determination of user access levels to information systems, locations, and ePHI, but not detailing all of the variables described above.

Education	Consider assigning an authorized user to approve access levels with information systems and locations that contain and use ePHI. If this is determined to not be reasonable and appropriate, document the reason why and implement a compensating control. 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.PS HPH CPG: 6 HICP: TV1 - Practice # 2, 10	Addressable	James Del Ciello	Sun Apr 06 12:18:14 PDT 2025

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 a person's access to the facility based on their role or function, but do not have additional validation requirements for access to our critical systems.
Education	Access to facilities, especially areas which house ePHI, should be limited to the minimum amount necessary for workforce members or visitors to complete their legitimate functions. Consider implementing procedures to validate a person's access to facilities based on their role. If this is determined to not be reasonable and appropriate, document the reason why and implement a compensating control. 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.AA, PR.IR, PR.DS, DE.CM, DE.CP, PR.PS HPH CPG: 6HICP: TV1 - Practice # 6	Addressable	James Del Ciello	Sun Apr 06 12:18:26 PDT 2025

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

Answer	We maintain lists of authorized persons but do not have controls in place to identify persons attempting to access the practice, grant access to authorized persons, or prevent access by unauthorized persons.
Education	Consider appropriate methods of validating access to your facility. Implement and document safeguards determined to be reasonable and appropriate. 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.AA, PR.IR, PR.DS, DE.CM, DE.CP HPH CPG: 6 HICP: TV1 - Practice # 6	Addressable	James Del Ciello	Sun Apr 06 12:18:51 PDT 2025

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	I don't know.
Education	Consider implementing procedures to validate a person's access to critical systems based on their role or function. If this is determined to not be reasonable and appropriate, document the reason why and implement a compensating control. Just as you might restrict physical access to different parts of your medical office, it is 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.AA, PR.IR, PR.DS, DE.CM, DE.CP, PR.PS HPH CPG: 6, 3 HICP: TV1 - Practice #3, 6	Addressable	James Del Ciello	Sun Apr 06 12:19:00 PDT 2025

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

Answer	I don't know.
Education	Consider implementing procedures to validate a third party person's access to facilities based on their role or function. If this is determined to not be reasonable and appropriate, document the reason why and implement a compensating control. Just as you might restrict physical access to different parts of your medical office, it is 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.AA, PR.IR, PR.DS, DE.CM, DE.CP, PR.PS HPH CPG: 6, 10 HICP: TV1 - Practice # 6	Addressable	James Del Ciello	Sun Apr 06 12:19:11 PDT 2025

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 allow the organization to centrally maintain and monitor access.

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.AA, PR.IR, PR.DS, DE.AE, DE.CM HPH CPG: 18 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:19:19 PDT 2025

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, DE.AE, DE.CM, PR.PS HPH CPG: 18 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:19:32 PDT 2025

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

Answer	No. We communicate and verbally authorize when repairs, modifications, or upgrades to the facility's physical security components are needed, but we do not have written procedures for this process.

Education	Consider including in your procedural documentation workforce members' roles and responsibilities as well as the authorization process for making repairs, modifications, and updates to your facility's physical security components. If this is determined to not be reasonable and appropriate, document the reason why and implement a compensating control.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(iv) NIST CSF: PR.DS, PR.MA HPH CPG: 11 HICP: N/A	Addressable	James Del Ciello	Sun Apr 06 12:19:50 PDT 2025

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, DE.AE, DE.CM, PR.DS HPH CPG: 11 HICP: TV1 - Practice # 5, 10	Addressable	James Del Ciello	Sun Apr 06 12:20:01 PDT 2025

Q18. Are electronic devices secured?

Answer	We secure electronic devices, but do not have documented procedures for these safeguards.
Education	Secure electronic devices with appropriate safeguards, such as screen guards, cable locks, locking storage rooms, cameras, and other physical features. Document these safeguards in your policies and procedures. 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.AA, PR.IR, PR.DS, DE.CM HPH CPG: 11, 16 HICP: TV1 - Practice # 2	Required	James Del Ciello	Sun Apr 06 12:20:13 PDT 2025

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

Answer	Yes. We manage our own backups of all critical ePHI (using portable storage devices) that enables continued access during device movement.
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.PS HPH CPG: 11, 16 HICP: TV1 - Practice # 4	Addressable	James Del Ciello	Sun Apr 06 12:20:24 PDT 2025

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

Answer	Yes. Devices are given to a third-party, which wipes the data and disposes of the devices appropriately 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. We are provided a certificate of destruction outlining the specific devices that were disposed of whenever this is performed.
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.AA, PR.IR, PR.DS, PR.PS HPH CPG: 11 HICP: TV1 - Practice # 5	Required	James Del Ciello	Sun Apr 06 12:20:45 PDT 2025

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.AA, PR.IR, PR.DS, DE.CM, ID.RA HPH CPG: 3, 11 HICP: TV1 - Practice # 4, 5	Required	James Del Ciello	Sun Apr 06 12:21:02 PDT 2025

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. Similarly, if an employee changes jobs within the organization, it is important to terminate access related to the employee's former position before granting access based on the requirements for the new position.		
References	**Compliance**	**Username**	**Audit Date**

HIPAA: §164.308(a)(3)(ii)(C) NIST CSF: PR.AA, PR.IR, PR.PS HPH CPG: 6 HICP: TV1 - Practice # 3	Addressable	James Del Ciello	Sun Apr 06 12:21:11 PDT 2025

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. Similarly, if an employee changes jobs within the organization, it is important to terminate access related to the employee's former position before granting access based on the requirements for the new position.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(C) NIST CSF: PR.AA, PR.IR, PR.PS HPH CPG: 10 HICP: TV1 - Practice # 3	Addressable	James Del Ciello	Sun Apr 06 12:21:20 PDT 2025

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

Answer	We delete files with ePHI from devices but do not do anything else to purge data prior to re-use.
Education	Deleting files does not fully purge data from the device. Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. 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.PS, PR.MA HPH CPG: 11, 16 HICP: TV1 - Practice # 4	Required	James Del Ciello	Sun Apr 06 12:21:38 PDT 2025

Section 6, Security and Business Associates Risk Score: 93 %

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: GV.RR, GV.PO, GV.OV HPH CPG: 10 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:21:50 PDT 2025

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

Answer	No.
Education	Working with business associates and third-party vendors can be beneficial to your practice, as long as reasonable and appropriate security precautions are taken for business associates accessing 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: N/A NIST CSF: GV.RR, GV.PO, GV.OV HPH CPG: 10 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:22:16 PDT 2025

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

Answer	I don't know. We have not formally considered which of our business associates require access to ePHI.

Education	Take an active role in protecting your ePHI. Review your business associate contracts to determine which business associates require a BAA and ensure fully executed BAAs are in place with all required business associates. 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.AA, PR.IR, PR.DS HPH CPG: 10, 12 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:22:26 PDT 2025

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

Answer	We do not consider degree of access as it pertains to business associates.
Education	Take an active role in protecting your ePHI. Determine the degree of access a business associate has by reviewing the amount of ePHI accessed, the types of devices and mechanisms used for access, and your ability to control and monitor their access. Document your procedures in your security policies. 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.AA, PR.IR, PR.DS, DE.CM HPH CPG: 10 HICP: TV1 - Practice # 3	Required	James Del Ciello	Sun Apr 06 12:22:44 PDT 2025

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

Answer	We are not sure how our business associates manage security or communicate changes to our practice.
Education	Consider including language in Business Associate Agreements describing their communication of relevant security changes to your practice.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.RR, GV.PO, GV.OV HPH CPG: 10, 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:23:10 PDT 2025

Q6. Have you executed business associate agreements with all business associates who create, receive, maintain, or transmit ePHI on your behalf?			
Answer	No. We do not execute BAAs when we have business associates accessing ePHI.		
Education	Make sure all business associates who access ePHI have a fully executed BAA with your practice before being granted access. Include this requirement in your security policies and procedures.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(3) NIST CSF: PR.AA, PR.IR HPH CPG: 10 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:23:22 PDT 2025

Q7. How do you maintain awareness of business associate security practices (i.e., in addition to Business Associate Agreements)?			
Answer	We are not sure how to maintain awareness of our business associates' security practices.		
Education	Consider monitoring, auditing, or obtaining information from business associates to ensure the security of ePHI and include language about this in Business Associate Agreements.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: N/A NIST CSF: PR.AT, RS.CO, DE.CM HPH CPG: 10, 12, 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:23:34 PDT 2025

Q8. Do you include satisfactory assurances within your Business Associate Agreements pertaining to how your business associates safeguard ePHI?			
Answer	No. We are not sure about what satisfactory assurances are included in our BAAs.		
Education	Ensure all BAAs have been updated to meet the requirements of the HIPAA Security Rule and Omnibus Rule updates to HIPAA.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.314(a)(1)(i) NIST CSF: GV.RR, GV.PO, GV.OV HPH CPG: 10, 12, 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:23:59 PDT 2025

Q9. What terms are in your BAAs to outline how your business associates ensure subcontractors access ePHI securely?	
Answer	We are not sure how to obtain satisfactory assurances from subcontractors.

Education	Ensure your practice can safeguard ePHI by ensuring the terms and conditions of your practice's BAAs outline appropriate requirements for your BAAs with subcontractors.

References	Compliance	Username	Audit Date
HIPAA: §164.314(a)(2)(iii) NIST CSF: DE.AE, RS.CO HPH CPG: 10 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:24:16 PDT 2025

Q10. Do your BAAs require your third-party vendors to report security incidents to your practice in a timely manner?

Answer	No. We are not sure how this requirement is described within our BAAs.
Education	Your practice may not be able to safeguard its information systems and ePHI if your practice's Business Associates are not required to provide satisfactory assurances for the protection of ePHI, obtain the same assurances from its subcontractors, and report security incidents (experienced by the Business Associate or its subcontractors) to you in a timely manner. Make sure your point of contact with your business associate knows whom to contact at your organization to provide information about security incidents.

References	Compliance	Username	Audit Date
HIPAA: §164.314(a)(2)(i)(c) NIST CSF: ID.RA, DE.AE, RS.CO HPH CPG: 10, 13 HICP: TV1 - Practice # 8	Required	James Del Ciello	Sun Apr 06 12:24:22 PDT 2025

Q11. Have you updated all your BAAs to reflect the requirements in the 2013 Omnibus Rule updates to HIPAA?

Answer	We assume all BAAs are up to date with the Omnibus Rule updates to HIPAA but have not reviewed the agreements to make sure.
Education	All BAAs should be reviewed to ensure compliance with the Omnibus Rule updates to HIPAA and HIPAA compliance.

References	Compliance	Username	Audit Date
HIPAA: §164.314(a)(1) NIST CSF: ID.AM, GV.OC, PR.AT, GV.RR, GV.PO, GV.OV HPH CPG: 10, 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:24:37 PDT 2025

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

Answer	We are not sure how these business associate relationships are documented.

Education	Knowing who provides services to your practice and the nature of the services is an important component of your security plan. Note that the Office for Civil Rights may request an inventory listing of your Business Associates in the event of an audit or investigation.

References	Compliance	Username	Audit Date
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS HPH CPG: 10 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:24:46 PDT 2025

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

Answer	No. We do not obtain assurances from business associates who access another covered entity's ePHI on our behalf.
Education	Make sure your practice has BAAs in place with covered entities for which your practice is a Business Associate as well as subcontractors to those covered entities who contract with your practice

References	Compliance	Username	Audit Date
HIPAA: §164.308(b)(2) NIST CSF: N/A HPH CPG: 10 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:25:00 PDT 2025

Q14. Does the organization require business associates and third-party vendors to implement security requirements more stringent than required in the HIPAA Rules?

Answer	No, contracts with vendors or BAs outline requirements to follow the HIPAA Rules as applicable to BAs without additional cybersecurity protocols.
Education	The HIPAA Rules require a covered entity to obtain satisfactory assurances from its business associate that it will appropriately safeguard PHI it receives or creates on behalf of the covered entity. Organizations could consider protocols within their business practice to include enhanced cybersecurity and supply chain requirements beyond those required by the HIPAA Rules that third parties can follow and how compliance with the requirements may be verified. Rules and protocols for information sharing between the organization and suppliers are detailed and included in contracts between the two.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.SC HPH CPG: 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:25:15 PDT 2025

Q15. How do you track and verify business associate and third-party vendor compliance to security policies and where are these policies documented?

Answer	The organization verifies business associate and third-party vendor status each year but does not perform evaluations.
Education	The organization could require business associates and third-party vendors to disclose cybersecurity features, functions, and known vulnerabilities of their products and services for the life of the product or the term of service. Contracts could require evidence of performing acceptable security practices through self-attestation, conformance to known standards, certifications, or inspections. Business associates and third-party vendors could be monitored to ensure they are fulfilling their security obligations throughout the relationship lifecycle.

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.SC HPH CPG: 13 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:25:27 PDT 2025

Section 7, Contingency Planning

Risk Score: 92 %

Threats & Vulnerabilities	Risk Rating

Section Questions

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

Answer	I don't know.
Education	Ensure your practice can operate effectively and efficiently under emergency by having a contingency plan. This should be included in your documented policies and procedures. The contingency plan should be reviewed, tested, and updated periodically. As part of this you should determine what critical services and ePHI must be available during an emergency. 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: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 7, 19 HICP: TV1 - Practice # 8	Required	James Del Ciello	Sun Apr 06 12:25:48 PDT 2025

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

Answer	I don't know.

Education	You should consider all natural and man-made disasters that could affect the confidentiality, integrity, and availability of ePHI. You should also document how you would respond in these situations to maintain security of ePHI in your policies and procedures.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA, ID.RA HPH CPG: 7, 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:25:56 PDT 2025

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.PS HPH CPG: 18, 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:26:06 PDT 2025

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

Answer	Our security incident response plan is tested as needed (for example, when activated in real-world situations) but not on a periodic basis.
Education	Consider documenting your incident response plan in your policies and procedures and testing the plan periodically using a documented process. The incident plan should cover broad categories of incidents to prepare for. Testing the incident plan is an effective means of preparation and training. 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.PS, RS.IP HPH CPG: 7, 18, 19 HICP: TV1 - Practice # 8	Required	James Del Ciello	Sun Apr 06 12:26:18 PDT 2025

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

Answer	I don't know.
Education	Identify workforce members who need access to facilities in the event of an emergency, identify roles and responsibilities, and create a backup plan for accessing facilities and critical data. 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, GV.RM, PR.PS, DE.AE, RS.MA, RS.CO, RS.AN, RS.MI, ID.AM, GV.RR, GV.PO, GV.OV HPH CPG: 7, 19 HICP: TV1 - Practice # 8	Required	James Del Ciello	Sun Apr 06 12:26:24 PDT 2025

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	I don't know.
Education	Consider evaluating all hardware and software systems, including those of business associates, to determine criticality of the systems and ePHI that would be accessed. Document this process and include all mission-critical systems in your contingency plan. 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: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 19 HICP: TV1 - Practice # 10	Required	James Del Ciello	Sun Apr 06 12:26:52 PDT 2025

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

Answer	I don't know.
Education	Document procedures to describe how your practice will maintain access to ePHI in the event of an emergency, system failure, or physical disaster. Your practice might not be able to recover ePHI and other health information during an emergency or when systems become unavailable if it does not backup ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage (e.g., cloud environment).

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(ii) NIST CSF: PR.AA, PR.IR, GV.OC, PR.DS, PR.PS, PR.MA, RS.MA, RS.CO HPH CPG: 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:26:57 PDT 2025

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

Answer I don't know.

Education Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(ii)(C) NIST CSF: GV.OC, GV.RM, PR.PS, RS.MA, RS.CO, RS.AN, RC.CO, RC.RP HPH CPG: 7, 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:27:00 PDT 2025

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

Answer I don't know.

Education You should establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Consider looking into whether your practice is implementing, documenting, and testing a data backup and restoration plan. 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: GV.OC, ID.RA, GV.RM, RS.AN, PR.PS, RS.MA, RS.CO, RC.CO, RC.RP, PR.DS HPH CPG: 19, 20 HICP: TV1 - Practice # 10	Required & Addressable	James Del Ciello	Sun Apr 06 12:27:07 PDT 2025

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

Answer I don't know.

Education	Details about how and when to activate should be documented in the emergency procedure.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(ii) NIST CSF: GV.OC, PR.PS, DE.AE, RS.MA, RS.CO HPH CPG: 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:27:12 PDT 2025

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

Answer	We do not have a written plan for accessing the facility in the event of disasters or emergency situations.
Education	Implement 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. Ensure members of the workforce who need access to the facility in an emergency have been identified. Define workforce member roles and responsibilities. Ensure that a backup plan for accessing the facility and critical data is in place.

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA, PR.DS, RS.CO, RC.RP HPH CPG: 19 HICP: N/A	Addressable	James Del Ciello	Sun Apr 06 12:27:24 PDT 2025

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

Answer	I don't know.
Education	Details about how and when to terminate should be documented in the emergency procedure.

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(2)(ii) NIST CSF: N/A HPH CPG: 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:27:36 PDT 2025

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

Answer	I don't know.
Education	Consider conducting technical and non-technical evaluations of security policies and procedures. This should be done periodically and in response to changes in the security environment.

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(8) NIST CSF: ID.AM, GV.OC, ID.RA, PR.PS, DE.AE, DE.CM, RS.MI, ID.IM, RC.MI HPH CPG: 19 HICP: N/A	Required	James Del Ciello	Sun Apr 06 12:27:43 PDT 2025

Practice Information (1 location)

Practice Name	TechNova
Address	443 27th Avenue East
City, State, Zip	Seattle, WA, 98112
Phone, Fax	206-650-2443
Point of Contact	James Del Ciello
Title/Role	Cybersecurity Network Administrator
Phone	206-650-2443
Email	jimdelciello@yahoo.com

Asset Information (0 total)

Risk	ID#	Type	Status	ePHI	Encryption	Assignment	Location

Business Associates and Vendors (0 total)

Vendor Name	Vendor Type	Satistfactory Assurances	Risk Assessed