Security Risk Assessment Tool

Application Version: 3.5.1

Detailed Report

Evergreen Valley Medical Center

05-04-2025

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.)	Low
	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	Critical
	Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions	Low
Unspecified workforce security responsibilities		
	Non-remediated weaknesses	Medium
	Prolonged duration of addressing non-remediated weaknesses	High
	Insider carelessness exposing ePHI or causing disruption to information systems and business processes	High

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	elieazer	Fri May 02 19:56:34 EDT 2025

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

Answer	We review the current regulations and do our best to meet them.
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	elieazer	Fri May 02 19:57:14 EDT 2025

Section 2, Security Policies

Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating
Inconsistent/unclear risk management documentation	
Unclear security coordination across workforce	Medium
Unstructured guidance for daily tasks and duties	High

Section Questions

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

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

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

HIPAA: §164.316(a) NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS HPH CPG: 1, 14, 15 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:41:08 EDT 2025

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.316(b)(2)(iii) NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS, ID.IM HPH CPG: 7, 14, 15, 19 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:41:36 EDT 2025

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

Answer	We have a periodic review of information security policies that formally evaluates their effectiveness. Policies and procedures are updated as needed.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.316(b)(2)(iii) NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS, ID.IM HPH CPG: 4 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:41:57 EDT 2025

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

Answer	Yes.

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(iii) NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS, ID.IM HPH CPG: 7, 15, 19 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:42:27 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(1)(i) & (ii) NIST CSF: GV.OC, GV.RM, PR.PS HPH CPG: 1, 15, 19 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:42:49 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.316(b)(2)(i) NIST CSF: GV.OC, GV.RM, PR.PS HPH CPG: 7, 18 HICP: N/A	Required	elieazer	Sat May 03 21:42:59 EDT 2025

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

Answer	Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.316(b)(2)(ii) NIST CSF: GV.OC, GV.RM, PR.PS HPH CPG: 4 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:43:13 EDT 2025

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

Answer	Appropriate workforce members receive instruction on our information security documentation and where to find it as part of their periodic privacy and security training. Documentation is securely made available to workforce members in physical or electronic formats.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Policies are established first and are then supplemented with procedures that enable the policies to be implemented. Policies describe what is expected, and procedures describe how the expectations are met.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.316(b)(2)(ii) NIST CSF: GV.OC, GV.RM, PR.PS, ID.RA HPH CPG: 4 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:45:36 EDT 2025

Section 3, Security & Workforce Risk Score: 16 %

Threats & Vulnerabilities	Risk Rating
Inadequate cybersecurity & IT training	
Information disclosure (ePHI, proprietary, intellectual, or confidential)	High
Disruption of business processes or information system function	High
Social engineering attack or email phishing attack	Medium

	Misuse of information systems and/or hardware	Low
	Information system or facility access granted to unauthorized personnel	Critical
	Installation of unauthorized software or applications	High
Failure to hold workforce members accountable for undesired actions		
	Insider carelessness causing disruption to computer systems	Low
	Insider carelessness exposing ePHI to unauthorized persons or entities	Critical
	Lack of interest for protecting sensitive information	High

Section Questions

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

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO, PR.PS, ID.AM HPH CPG: 4 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:47:32 EDT 2025

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

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

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

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

HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO, PR.PS HPH CPG: 4 HICP: TV1 - Practice # 10	Required	elieazer	Sat May 03 21:47:41 EDT 2025

Q3. Is your security officer qualified for the position?

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO HPH CPG: N/A HICP: TV1 - Practice # 8	Required	elieazer	Sat May 03 21:49:04 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO HPH CPG: 4 HICP: N/A	Required	elieazer	Sat May 03 21:49:13 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.AE, GV.RR, RS.CO HPH CPG: 4 HICP: N/A	Required	elieazer	Sat May 03 21:49:27 EDT 2025

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

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(A) NIST CSF: ID.AM, PR.MA, DE.CM, DE.AE, PR.PS HPH CPG: 6, 7 HICP: TV1 - Practice #2, 3	Required	elieazer	Sat May 03 21:49:37 EDT 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 Yes.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(ii)(B) NIST CSF: DE.AE, PR.AA, PR.IR, PR.PS HPH CPG: 6 HICP: N/A	Addressable	elieazer	Sat May 03 21:50:04 EDT 2025

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

Answer Professional references are collected and verified along with licenses, credentials, and certifications. We do not perform criminal background checks.

Education Consider which methods of personnel screening are reasonable and appropriate for your organization in order to verify the trustworthiness of workforce members who will access 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	elieazer	Sat May 03 21:50:19 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT , GV.RM, PR.PS HPH CPG: 4 HICP: TV1 - Practice # 1, 4	Required	elieazer	Sat May 03 21:50:30 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT, PR.PS HPH CPG: 4 HICP: TV1 - Practice # 1, 4, 10	Required	elieazer	Sat May 03 21:50:54 EDT 2025

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

Answer

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(i) NIST CSF: PR.AT, PR.PS HPH CPG: 4 HICP: N/A	Required	elieazer	Sat May 03 21:51:00 EDT 2025

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

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(ii)(C) NIST CSF: DE.AE, DE.CM, RS.CO, PR.AT, PR.PS HPH CPG: 18 HICP: TV1 - Practice #2, 3	Addressable	elieazer	Sat May 03 21:51:21 EDT 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	elieazer	Sat May 03 21:52:52 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(ii)(D) NIST CSF: PR.AT HPH CPG: 2, 8 HICP: TV1 - Practice # 2, 3	Addressable	elieazer	Sat May 03 21:57:41 EDT 2025

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

Answer

Yes.

Education

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

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(5)(ii)(A) NIST CSF: PR.AT, ID.RA, GV.OC, GV.RR, GV.PO, GV.OV HPH CPG: 4 HICP: TV1 - Practice # 1, 4	Addressable	elieazer	Sat May 03 21:58:45 EDT 2025

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(5)(ii)(A) NIST CSF: PR.AT, ID.RA, GV.OC, GV.RR, GV.PO, GV.OV HPH CPG: 4 HICP: TV1 - Practice # 1, 4	Addressable	elieazer	Sat May 03 21:59:28 EDT 2025

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(1)(ii)(C) NIST CSF: PR.PS HPH CPG: N/A HICP: N/A	Required	elieazer	Sat May 03 22:16:15 EDT 2025

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

Answer	Formal written documentation of the sanction and the reason for the sanction.
Education	Consider which sanction policies and procedures are reasonable and appropriate for your organization in order to hold personnel accountable if they do not follow your security policies and procedures.

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(1)(ii)(C) NIST CSF: PR.AT, RS.CO, PR.PS HPH CPG: N/A HICP: N/A	Required	elieazer	Sat May 03 22:24:41 EDT 2025

Section 4, Security & Data		Risk Score: 10 %
Threats & Vulnerabilities		Risk Rating
Inadequate use of encryption for ePHI		
	Disclosure of passwords or login information	High
	Information disclosure, loss, or theft (ePHI, proprietary, intellectual, or confidential)	Medium
	Fines from regulatory enforcement (due to lack of encryption safe harbor)	Critical
	Information system access granted to unauthorized personnel	Low
	Unauthorized access to or modification of ePHI/sensitive information	Critical
Inadequate integrity verification of ePHI		
	Accidental modification to ePHI	Critical
	Damage to public reputation via misuse of patient chart data	Critical
	Inaccurate information given to patients or providers	Critical
	Unauthorized modification to ePHI	High
ePHI in transit lacking encryption		
	Information disclosure or theft (ePHI, proprietary, intellectual, or confidential)	High
	Unauthorized access to or modification of ePHI/sensitive information	High
	Fines from regulatory enforcement (due to lack of encryption safe harbor)	Critical

Section Questions

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

Answer	Yes.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.PS, PR.AA, PR.IR HPH CPG: 6 HICP: TV1 - Practice #2, 3	Required	elieazer	Sat May 03 23:03:38 EDT 2025

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

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.PS, PR.AA, PR.IRHPH CPG: 3, 6 HICP: TV1 - Practice #2, 3	Required	elieazer	Sat May 03 23:03:59 EDT 2025

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

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

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

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) NIST CSF: PR.AA, PR.IR, PR.PS HPH CPG: 6 HICP: TV1 - Practice # 3	Addressable	elieazer	Sat May 03 23:04:16 EDT 2025

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

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.502(b) NIST CSF: PR.AA, PR.IR, PR.PS, GV.RM, PR.DS HPH CPG: 3, 9 HICP: TV1 - Practice # 3	Required	elieazer	Sat May 03 23:04:29 EDT 2025

Q5. How are individual users identified when accessing ePHI?

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(i) NIST CSF: PR.AA, PR.IR, DE.CM HPH CPG: 8, 9 HICP: TV1 - Practice # 3	Required	elieazer	Sat May 03 23:05:01 EDT 2025

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

Answer Yes. We have written procedures to ensure workforce members' access privileges are minimum necessary but these are not always based on their roles.

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	elieazer	Sat May 03 23:07:03 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(3)(i) NIST CSF: PR.AT, PR.PS, DE.CMHPH CPG: 3, 8, 9 HICP: TV1 - Practice # 3,4	Required	elieazer	Sat May 03 23:07:19 EDT 2025

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

Answer

Yes.

Education

This is the most effective option. Whenever reasonable and appropriate implement a mechanism to encrypt and decrypt ePHI. Install encryption software on every endpoint that connects to your EHR system, especially mobile devices such as laptops. Maintain audit trails of this encryption in case a device is ever lost or stolen. This simple and inexpensive precaution may prevent a complicated and expensive breach. If supported by the manufacturer, medical devices should have local encryption enabled in case the device is stolen. Implement an e-mail encryption module that enables users to securely send e-mails to 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	elieazer	Sat May 03 23:08:20 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(2)(ii) NIST CSF: PR.AA, PR.IR, PR.DS, PR.PS HPH CPG: 5 HICP: TV1 - Practice # 1, 4	Addressable	elieazer	Sat May 03 23:38:42 EDT 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	elieazer	Sat May 03 23:39:14 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: PR.DS HPH CPG: 5 HICP: TV1 - Practice # 2	Addressable	elieazer	Sat May 03 23:39:29 EDT 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

All of the above.

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(e)(2)(ii) NIST CSF: PR.AA, PR.IR, PR.DS, DE.CM, ID.RA, GV.RM HPH CPG: 5 HICP: TV1 - Practice # 2	Addressable	elieazer	Sat May 03 23:39:45 EDT 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	All of the above.
Education	Encryption in these areas is critical to protecting ePHI in your cloud environments. Contracts with EHR vendors should include language that requires medical/PHI data to be encrypted both at rest and during transmission between systems.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(e)(2)(ii) NIST CSF: N/A HPH CPG: 5 HICP: TV1 - Practice # 1	Addressable	elieazer	Sat May 03 23:39:52 EDT 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	All of the above.
Education	Encryption in these areas is critical to protecting ePHI in transit. 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	elieazer	Sat May 03 23:40:06 EDT 2025

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

Answer	Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, rendering it more difficult for hackers to maintain programs that are aligned with the most current version of that software application. Configure endpoints to patch automatically and ensure that third-party applications (e.g., Adobe Flash) are patched as soon as possible. Schedule and conduct vulnerability scans on servers and systems under your control 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	elieazer	Sat May 03 23:40:23 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(a)(1) NIST CSF: PR.AA, PR.IR, PR.DS, PR.PS, ID.RA, PR.MA, DE.CM HPH CPG: 1, 18, 20 HICP: TV1 - Practice # 7	Required	elieazer	Sun May 04 17:09:19 EDT 2025

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(b) NIST CSF: PR.DS, DE.CM HPH CPG: 14, 15, 16, 18, 20 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:09:36 EDT 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	elieazer	Sun May 04 17:09:44 EDT 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	elieazer	Sun May 04 17:11:40 EDT 2025

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

Answer	Yes, automatic logoff is enabled on all devices and platforms to terminate access to ePHI after a set time of inactivity.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Configure systems and endpoints to automatically lock and log off users after a predetermined period of inactivity, such as 15 minutes.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(iii) NIST CSF: PR.AA, PR.IR, PR.DS HPH CPG: 11 HICP: TV1 - Practice # 3	Addressable	elieazer	Sun May 04 17:11:51 EDT 2025

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(d) NIST CSF: PR.AA, PR.IR, PR.DS, PR.MA, DE.CM HPH CPG: 3, 8 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:12:01 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(d) NIST CSF: PR.AA, PR.IR, PR.DS, PR.MA, DE.CM HPH CPG: 3, 8 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:12:23 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.312(d) NIST CSF: PR.AA, PR.IR, PR.DS, PR.MA, DE.CM, PR.PS HPH CPG: 3, 8 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:13:11 EDT 2025

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

Answer

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

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of 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	elieazer	Sun May 04 17:16:44 EDT 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	elieazer	Sun May 04 17:18:43 EDT 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	elieazer	Sun May 04 17:19:11 EDT 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	elieazer	Sun May 04 17:19:35 EDT 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	elieazer	Sun May 04 17:19:52 EDT 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, vulnerability scans or penetration testing are done but only on a as needed basis such as when there is a suspected weakness.

Education	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	elieazer	Sun May 04 17:20:27 EDT 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	elieazer	Sun May 04 17:20:40 EDT 2025

Section 5, Security and the Practice Risk Score: 4 %

Threats & Vulnerabilities		Risk Rating
Undocumented location of equipment or assets		
	Unconfirmed identity of connected physical devices/equipment	High
	Unauthorized devices gaining access to the network	Medium
	Unconfirmed identity of connected devices/equipment	Low
	Exploitation of unsecured computer systems	High
Inadequate sanitation of media		

	Information disclosure or theft (ePHI, proprietary, intellectual, or confidential)	Critical
	Disclosure of passwords and or login information	Medium
	Unauthorized access to ePHI/sensitive information	Medium
	Unknown disposition of unused devices and data	Medium
	Unauthorized modification of user accounts and/or permissions	High

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	elieazer	Sun May 04 17:24:56 EDT 2025

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

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(ii) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 7, 16 HICP: TV1 - Practice # 6	Addressable	elieazer	Sun May 04 17:29:54 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(1) NIST CSF: ID.RA, PR.AA, PR.IR, DE.CM, PR.PS HPH CPG: 7, 11 HICP: TV1 - Practice # 6	Required	elieazer	Sun May 04 17:30:07 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.310(b) NIST CSF: PR.AA, PR.IR, PR.DS, DE.CM, PR.PS HPH CPG: 10, 6 HICP: TV1 - Practice #4, 6	Required	elieazer	Sun May 04 17:30:17 EDT 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 physical protections in place for all electronic devices and this is documented in policy and procedure.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Examples include installation of anti-theft cables, locks on rooms where the devices are located, 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	elieazer	Sun May 04 17:30:34 EDT 2025

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

Answer

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

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.310(c) NIST CSF: PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 11 HICP: TV1 - Practice # 2, 6	Required	elieazer	Sun May 04 17:30:59 EDT 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	elieazer	Sun May 04 17:31:10 EDT 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 outlining who has the authorization to approve access to information systems, location, and ePHI; how access requests are submitted; and how access is granted.

Education

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

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(3)(ii)(A) NIST CSF: ID.AM, PR.MA, PR.PS HPH CPG: 6 HICP: TV1 - Practice # 2, 10	Addressable	elieazer	Sun May 04 17:31:31 EDT 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 access to our facility. Access levels are based on role or function. We also have strict requirements for validating workforce members or visitors who seek access to our critical systems and software programs.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as network devices need to be secured, physical access to the server and network equipment should be restricted to IT professionals. Configure physical rooms and wireless networks to allow internet access only.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AA, PR.IR, PR.DS, DE.CM, DE.CP, PR.PS HPH CPG: 6HICP: TV1 - Practice # 6	Addressable	elieazer	Sun May 04 17:31:37 EDT 2025

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

Answer	We maintain lists of authorized persons and have controls in place to identify persons attempting to access the practice, grant access to authorized persons, and prevent access by unauthorized persons.
Education	These are effective means of validating facility access. Always keep data and network closets locked. Grant access using badge readers rather than traditional key locks.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AA, PR.IR, PR.DS, DE.CM, DE.CP HPH CPG: 6 HICP: TV1 - Practice # 6	Addressable	elieazer	Sun May 04 17:31:49 EDT 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	Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as you might restrict physical access to different parts of your medical office, it 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	elieazer	Sun May 04 17:32:13 EDT 2025

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

Answer

Yes.

Education

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

References	Compliance	Username	Audit Date
HIPAA: §164.310(a)(2)(iii) NIST CSF: ID.RA, PR.AA, PR.IR, PR.DS, DE.CM, DE.CP HPH CPG: 6, 3 HICP:TV1, Practice # 2	Addressable	elieazer	Sun May 04 17:32:23 EDT 2025

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

Answer

Yes.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Just as you might restrict physical access to different parts of your medical office, it 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	elieazer	Sun May 04 17:32:50 EDT 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	elieazer	Sun May 04 17:33:26 EDT 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	elieazer	Sun May 04 17:33:39 EDT 2025

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

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

Education Consider including in your procedural documentation what your workforce members' roles and responsibilities are in the repair and modification of physical security components within your facility.
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	elieazer	Sun May 04 17:35:18 EDT 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	elieazer	Sun May 04 17:35:28 EDT 2025

Q18. Are electronic devices secured?

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

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

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

HIPAA: §164.310(c) NIST CSF: PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 11, 16 HICP: TV1 - Practice # 2	Required	elieazer	Sun May 04 17:35:35 EDT 2025

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

Answer	Yes. Our critical data and ePHI is centrally stored (such as in a cloud or active directory server) that can be accessed from any authorized device.
Education	This is an effective option to protect the confidentiality, integrity, and availability of ePHI. Make sure backups will be available and functional when needed through periodic testing. Train staff never to back up data on uncontrolled storage devices or personal cloud services. Leveraging the cloud for backup purposes is acceptable if you have established an agreement with the cloud vendor and verified the security of the vendor's systems.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(d)(2)(iv) NIST CSF: PR.DS, PR.PS HPH CPG: 11, 16 HICP: TV1 - Practice # 4	Addressable	elieazer	Sun May 04 17:35:40 EDT 2025

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

Answer	Yes. We remove any data storage or memory component from the device and then store it in a secure location. Data is wiped from the device prior to disposing of the device using a method that conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Although it can be difficult to implement and sustain IT asset management processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(d)(1) NIST CSF: PR.AA, PR.IR, PR.DS, PR.PS HPH CPG: 11 HICP: TV1 - Practice # 5	Required	elieazer	Sun May 04 17:37:30 EDT 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	elieazer	Sun May 04 17:38:15 EDT 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	elieazer	Sun May 04 17:38:27 EDT 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	elieazer	Sun May 04 17:38:33 EDT 2025

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

Answer	We have a process to completely purge data from all devices prior to re-use through device reimaging, degaussing, or other industry standard method; our method conforms to guidelines in NIST SP 800-88 and OCR Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
Education	This is an effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Ensure that obsolete data are removed or destroyed properly so they cannot be accessed by cyber-thieves. Just as paper medical and financial records must be fully destroyed by shredding or burning, digital data must be properly disposed of to ensure that they cannot be inappropriately recovered. Discuss options for properly disposing of outdated or unneeded data with your IT support. Do not assume that deleting or erasing files means that the data are destroyed.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(d)(2)(ii) NIST CSF: PR.PS, PR.MA HPH CPG: 11, 16 HICP: TV1 - Practice # 4	Required	elieazer	Sun May 04 17:38:53 EDT 2025

Section 6, Security and Business Associates

Risk Score: 13 %

Threats & Vulnerabilities		Risk Rating
Uncontrolled access to ePHI to business associates/vendors		
	Access to unauthorized segments of the network	Low
	Carelessness causing disruption to computer systems	Medium
	Carelessness exposing ePHI	High
	Damage to public reputation due to breach	High
	Disclosure of passwords and or login information	Low
	ePHI accessed by unauthorized entities	Medium
	Exploiting unpatched systems and software	Medium
	Unauthorized access to ePHI	Low
	Unauthorized modification to ePHI	High

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	elieazer	Sun May 04 17:54:06 EDT 2025

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

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

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

HIPAA: N/A NIST CSF: GV.RR, GV.PO, GV.OV HPH CPG: 10 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:54:25 EDT 2025

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

Answer	We review business associate contracts to determine which vendors or contractors require access to ePHI and we include a Business Associate Agreement (BAA) in our contract with them.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. As user accounts are established, the accounts must be granted access to the organization's computers and programs, as appropriate to each user. Consider following the "minimum necessary" principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization. This limits the organization's exposure to unauthorized access, loss, and theft of data if the user's identity or access is compromised.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS HPH CPG: 10, 12 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:54:39 EDT 2025

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

Answer	We determine degree of access based on the amount of ePHI accessed, the types of devices or mechanisms used for access, and our ability to control and monitor third-party access.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Implement access management procedures to track and monitor user access to computers and programs.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS, DE.CM HPH CPG: 10 HICP: TV1 - Practice # 3	Required	elieazer	Sun May 04 17:54:53 EDT 2025

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

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

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

References	Compliance	Username	Audit Date
HIPAA: N/A NIST CSF: GV.RR, GV.PO, GV.OV HPH CPG: 10, 13 HICP: N/A	Required	elieazer	Sun May 04 17:55:13 EDT 2025

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

Answer	Yes. We ensure all business associates have a fully executed BAA with us before creating, receiving, maintaining, or transmitting ePHI on our behalf.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	Compliance	Username	Audit Date
HIPAA: §164.308(b)(3) NIST CSF: PR.AA, PR.IR HPH CPG: 10 HICP: N/A	Required	elieazer	Sun May 04 17:55:22 EDT 2025

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

Answer	We rely on the language of our BAAs to ensure that business associates are securing ePHI.
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	elieazer	Sun May 04 17:55:31 EDT 2025

Q8. Do you include satisfactory assurances within your Business Associate Agreements pertaining to how your business associates safeguard ePHI?

Answer	Yes. BAAs include specifications on authorized use and disclosure of ePHI.
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	elieazer	Sun May 04 17:55:59 EDT 2025

Q9. What terms are in your BAAs to outline how your business associates ensure subcontractors access ePHI securely?

Answer In addition to language in our BAAs, our Business Associates provide specific assurances to us, including how they ensure subcontractors secure ePHI.

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

References	Compliance	Username	Audit Date
HIPAA: §164.314(a)(2)(iii) NIST CSF: DE.AE, RS.CO HPH CPG: 10 HICP: N/A	Required	elieazer	Sun May 04 17:56:24 EDT 2025

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

Answer Yes. Our BAAs describe requirements 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 our practice in a timely manner.

Education This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. 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	elieazer	Sun May 04 17:56:37 EDT 2025

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

Answer We have reviewed all BAAs and have confirmed their compliance with the Omnibus Rule updates to HIPAA.

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: §164.314(a)(1) NIST CSF: ID.AM, GV.OC, PR.AT, GV.RR, GV.PO, GV.OV HPH CPG: 10, 13 HICP: N/A	Required	elieazer	Sun May 04 18:01:07 EDT 2025

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

Answer	We maintain a current listing of all business associates with access to ePHI in addition to having Business Associate Agreements (BAAs) on file with any business associates with access to ePHI.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(1) NIST CSF: ID.AM, PR.AA, PR.IR, PR.DS HPH CPG: 10 HICP: N/A	Required	elieazer	Sun May 04 18:01:13 EDT 2025

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

Answer	Yes. We make sure to have BAAs in place with covered entities for which we are Business Associates as well as subcontractors to those covered entities who contract with us.
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(2) NIST CSF: N/A HPH CPG: 10 HICP: N/A	Required	elieazer	Sun May 04 18:01:18 EDT 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	Yes, contracts with vendors or BAs outline requirements to follow the HIPAA Rules as applicable to BAs with additional cybersecurity protocols.

Education	This is the most effective of the options provided. The HIPAA Rules require a covered entity obtain satisfactory assurances from its business associates 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	elieazer	Sun May 04 18:01:37 EDT 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 has developed a risk management program with policies and procedures that guide the implementation and monitoring of business associate and third-party vendor activities related to cybersecurity compliance.
Education	This is the most effective of the options provided. The organization could require business associate and third-party vendor 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	elieazer	Sun May 04 18:01:44 EDT 2025

Section 7, Contingency Planning Risk Score: 10 %

Threats & Vulnerabilities	Risk Rating
Lack of consideration to reasonably anticipated environmental threats	
Damage to public reputation due to information breach/loss	High
Physical damage to facility	Critical
Financial loss from increased downtime of information systems	High

	Inability to recovery from system failure	Critical
	Increased recovery time during unexpected downtime of information systems	Critical
	Injury or death of personnel (employee, patient, guest)	Medium
	Loss of productivity	Medium
	Overheating of network devices due to increased ambient temperature	Medium
	Physical access granted to unauthorized persons or entities	Low
	Power outage affecting the availability of critical security and information systems	High

Section Questions

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

Answer	Yes.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 7, 19 HICP: TV1 - Practice # 8	Required	elieazer	Sun May 04 18:04:39 EDT 2025

Q2. Is your contingency plan documented?

Answer	Yes.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:04:46 EDT 2025

Q3. Do you periodically update your contingency plan?

Answer Yes.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA, ID.IM HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:04:58 EDT 2025

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

Answer We periodically review the plans contents, perform tests of the plan, and record the results. We revise the plan as needed and document this in policy.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(ii)(D) NIST CSF: ID.IM, ID.RA, PR.PS, GV.OC HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:05:04 EDT 2025

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

Answer Yes.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA, ID.RA HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:05:12 EDT 2025

Q6. What types of emergencies have you considered?

Answer We have considered natural disasters, such as wildfire, damaging winds, floods, hurricanes, tornadoes, or earthquakes.

Education	You should consider infrastructure and man-made disasters that could affect the confidentiality, integrity, and availability of ePHI.		
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	elieazer	Sun May 04 18:05:18 EDT 2025

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

Answer	Yes.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:05:30 EDT 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	elieazer	Sun May 04 18:05:35 EDT 2025

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

Answer	We have a security incident response plan documented in our policies and procedures.

Education Consider testing the security incident response 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	elieazer	Sun May 04 18:06:05 EDT 2025

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

Answer Yes.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(6)(ii) NIST CSF: RC.CO, 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	elieazer	Sun May 04 18:06:45 EDT 2025

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

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

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

References	Compliance	Username	Audit Date

HIPAA: §164.308(a)(6)(ii) NIST CSF: PR.AT, RC.CO, GV.RM, PR.PS, DE.AE, RS.MA, RS.CO, RS.AN, RS.MI, ID.AM, ID.RA HPH CPG: 4, 7, 19 HICP: TV1 - Practice # 8	Required	elieazer	Sun May 04 18:06:53 EDT 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

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

Education

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(7)(i) NIST CSF: GV.OC, GV.RM, PR.AA, PR.IR, PR.PS, RS.MA HPH CPG: 19 HICP: TV1 - Practice # 10	Required	elieazer	Sun May 04 18:07:03 EDT 2025

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

Answer

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

Education

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(ii) NIST CSF: PR.AA, PR.IR, GV.OC, PR.DS, PR.PS, PR.MA, RS.MA, RS.CO HPH CPG: 19 HICP: N/A	Required	elieazer	Sun May 04 18:07:10 EDT 2025

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

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

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(ii)(C) NIST CSF: GV.OC, GV.RM, PR.PS, RS.MA, RS.CO, RS.AN, RC.CO, RC.RP HPH CPG: 7, 19 HICP: N/A	Required	elieazer	Sun May 04 18:07:20 EDT 2025

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

Answer Yes, we have a plan for determining which data is critically needed, creating retrievable, exact copies of critical data and how to restore that data, including from alternate locations. We also test and revise the plan, as needed.

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

References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(7)(ii)(A),§164.308(a)(7)(ii)(B), and §164.308(a)(7)(ii)(E) NIST CSF: 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	elieazer	Sun May 04 18:07:31 EDT 2025

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

Answer Upon identification or initiation of an emergency situation, emergency procedures are activated according to documented procedure, such as by formal communication from the security officer or other designated personnel.

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

References	Compliance	Username	Audit Date

HIPAA: §164.312(a)(2)(ii) NIST CSF: GV.OC, PR.PS, DE.AE, RS.MA, RS.CO HPH CPG: 19 HICP: N/A	Required	elieazer	Sun May 04 18:07:45 EDT 2025

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

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.310(a)(2)(i) NIST CSF: 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	elieazer	Sun May 04 18:07:58 EDT 2025

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

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

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.312(a)(2)(ii) NIST CSF: N/A HPH CPG: 19 HICP: N/A	Required	elieazer	Sun May 04 18:08:12 EDT 2025

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

Answer Yes.

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

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

HIPAA: §164.308(a)(8) NIST CSF: ID.AM, GV.OC, ID.RA, PR.PS, DE.AE, DE.CM, RS.MI, ID.IM, RC.MI HPH CPG: 19 HICP: N/A	Required	elieazer	Sun May 04 18:08:27 EDT 2025

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

Answer

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

Education

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

References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(8) NIST CSF: ID.AM, GV.OC, ID.RA, PR.PS, DE.AE, DE.CM, RS.MI, ID.IM, RC.MI HPH CPG: 19 HICP: N/A	Required	elieazer	Sun May 04 18:09:05 EDT 2025

Practice Information (1 location)

Practice Name	Evergreen Valley Medical Center
Address	1000 Evergreen Parkway,
City, State, Zip	Chaster, NY, 12520
Phone, Fax	(845) 555-0100
Point of Contact	Alice Thompson
Title/Role	Director of IT
Phone	(845) 555-0150
Email	alice.thompson@evergreenchasterny.org

Asset Information (16 total)

Risk	ID#	Type	Status	ePHI	Encryption	Assignment	Location
No	LLM-SRV- 01	Server	Active	No	Yes	LLM Model Server (De-identified)	Main Data Center
No	LLM-GW-0 1	Server	Active	Yes	Yes	LLM Runtime Access Gateway	Main Data Center
No	LLM-FS-0 1	File Server	Active	No	Yes	De-identified Case Knowledge Base	Main Data Center
No	LLM-FS-0 2	File Server	Active	Yes	Yes	Patient-Specific PHI Storage	Main Data Center
No	LLM-AC-0 1	Access Control System	Active	No	Yes	Session-Based PHI Authorization	Main Data Center
No	LLM-LOG- 01	Logging System	Active	Possibly	Yes	LLM Audit Logging	Main Data Center
No	LLM-API- 01	API Gateway	Active	Yes	Yes	LLM API Gateway	Main Data Center
No	LLM-RP-0 1	Reverse Proxy	Active	Yes	Yes	LLM Reverse Proxy	Main Data Center
No	LLM-MGMT -01	Model Management	Active	No	Yes	LLM Version Controller	Main Data Center
No	LLM-MON- 01	Monitoring System	Active	Possibly	Yes	LLM Behavioral Monitoring System	Main Data Center
No	LLM-POL- 01	Policy Repository	Active	No	Yes	Prompt Control Policies	Main Data Center
No	LLM-CONS ENT-01	Consent Manager	Active	Yes	Yes	Patient Consent Verification Tool	Main Data Center
No	LLM-QA-0 1	Validation Server	Active	No	Yes	Model Output QA System	Staging/Test Environment

Risk	ID#	Type	Status	ePHI	Encryption	Assignment	Location
No	LLM-SIM- 01	Simulation Engine	Active	No	Yes	Synthetic Patient Generator	Staging/Test Environment
No	LLM-DEID -01	De-ID Pipeline	Active	Yes	Yes	PHI Stripping Pipeline	Data Engineering Node
No	LLM-PROM PT-01	Prompt Builder	Active	Yes	Yes	Clinical Prompt Assembly Service	Main Data Center

Business Associates and Vendors (1 total)

Vendor Name	Vendor Type	Satistfactory Assurances	Risk Assessed
MedIncept AI Systems, Inc.		false	false