
# U.S. Department of Health and Human Services (HHS)
# The Office of the National Coordinator for Health Information Technology (ONC)

# Security Risk Assessment (SRA) Tool
# Technical Safeguards Content

---

**Version Date: September 2016**

**DISCLAIMER**

The Security Risk Assessment Tool at 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: 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. They are not required for compliance with the HIPAA Security Rule's risk assessment and risk management standards. 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.

# Contents

## Acronym Index

| Acronym | Definition |
|---|---|
| CD | Compact Disk |
| CERT | Community Emergency Response Team |
| CFR | Code of Federal Regulations |
| CISA | Certified Information Systems Auditor |
| CISSP | Certified Information Systems Security Professional |
| EHR | Electronic Health Record |
| ePHI | Electronic Protected Health Information |
| HHS | U.S. Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OCR | The Office for Civil Rights within HHS |
| ONC | The Office of the National Coordinator for Health Information Technology within HHS |
| PHI | Protected Health Information |
| RBAC | Role-based Access Control |
| SRA | Security Risk Assessment |
| SRA Tool | Security Risk Assessment Tool |
| USB | Universal Serial Bus |

## How to Use this Document

The HIPAA Security Rule requires health care providers, health plans and business associates to conduct risk analyses and implement technical, physical and administrative safeguards for ePHI. The HHS Office for Civil Rights (OCR) enforces the HIPAA Security Rule, which in turn requires HIPAA regulated entities to regularly assess the security risks of their processes and systems. In conjunction with OCR, the Office of the National Coordinator for Health IT (ONC), developed this risk assessment guide, to help providers and other HIPAA regulated entities protect ePHI through technical safeguards. Technical safeguards include hardware, software, and other technology that limits access to ePHI. Examples of the technical safeguards required by the HIPAA Security Rule include the following:

- Access controls to restrict access to ePHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper ePHI alteration or destruction
- Transmission security measures to protect ePHI when transmitted over an electronic network

This document is a paper-based version of the Security Risk Assessment Tool, a free on-line tool. To use the paper-based version of the tool, complete the following questions. Each question will help you think through a certain aspect of your security program. For each question:

1. Consider the threats and vulnerabilities to your IT systems and programs. Consult the "Threats and Vulnerabilities" portion of the question to brainstorm potential threats you may have missed.
2. Document your current activities in the box provided.
3. If you current activities do not address all the threats and vulnerabilities you have identified, develop and document a remediation plan in the box provided.
4. Document the impact and likelihood of any unaddressed threats and vulnerabilities. Not all risks can be reduced to zero (aka, no risk); your organization may be comfortable accepting some level of risk. If so, document the impact and likelihood of this residual risk as well.
5. Lastly, calculate an overall risk score for the question. You are free to use your own risk-rating method, but a common method uses impact and likelihood to determine overall risk using this matrix:

| | Likelihood | | | |
|---|---|---|---|---|
| Impact | | Low | Medium | High |
| | Low | Low Risk | Low Risk | Low Risk |
| | Medium | Low Risk | Medium Risk | Medium Risk |
| | High | Low Risk | Medium Risk | High Risk |

If, after completing all of the questions, threats and vulnerabilities still exist but are unaccounted for (i.e., a particular threat or vulnerability did not fit well with any of the existing questions), you should identify those unaccounted for threats and vulnerabilities, append them to the end of this document and assess the risk to your e-PHI by following the steps above. When you have completed the entire assessment, review you overall risks, prioritizing the "high" and "medium" risks first, particularly those that are unaddressed by your current activities, and take appropriate steps to remediate identified risks. Neither the paper tool nor the on-line tool prescribe how to remediate a risk. You will have to make decisions on remediation that are appropriate for the risks you identified for your organization.

Additional information on performing security risk analysis may be found at the HHS Office for Civil Rights website,[1] HealthIT.gov,[2] and in NIST Special Publication 800-30 Guide for Conducting Risk Assessments.[3]

## Why you should use this Tool?

Appropriately securing your ePHI is not only legally required under HIPAA, but also is important for the safety of your patients, and for your business reputation. Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI. For example,

- If through lack of security controls a malicious criminal accesses your system and takes it hostage, you may have no data available to care for your patients.
- If through lack of training and education, your staff does not keep information about patient's confidential, your patients could be upset
- If though lack of security controls, the accuracy of your ePHI is compromised and loses integrity, the quality of the care you deliver could be impacted.

These three goals: availability, confidentiality and integrity are the reasons why appropriately securing ePHI for which you are responsible is legally required. Underneath these important concepts are the details of how effectively your policies, procedures, staff education, and security controls work. Using this took will help you identify specific areas to focus your attention in improving how you secure ePHI. While ONC does require that Certified EHR Technology have certain security features built in, for some

[1] http://www.hhs.gov/hipaa/index.html
[2] https://www.healthit.gov/
[3] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

of these features, you need to take advantage of them, sort of like a seat belt in a car: every car has seatbelts, but you need to buckle them. This tool will help you identify those areas where you need to "buckle up."

**T1 - §164.312(a)(1) Standard** Does your practice have policies and procedures requiring safeguards to limit access to ePHI to those persons and software programs appropriate for their role?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, Waverly has policies and procedures regarding segregating functions and limiting access to information, hard copy charts, EHR, and how it is removed upon termination. Segregating access to systems based upon job title or role.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.
- Support the available automated security features of Certified EHR Technology, if you use CEHRT.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies and procedures for limiting access to ePHI, then those without a need to know may be able to access your ePHI.

Some potential impacts include:

- Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
[45 CFR §164.312(a)(1)]

Develop, document, and disseminate and enforce to workforce members an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the access control policy and associated access controls.
[NIST SP 800-53 AC-1]

**T2 - § 164.312(a)(1) Standard** Does your practice have policies and procedures to grant access to ePHI based on the person or software programs appropriate for their role?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, Waverly has policies and procedures regarding segregating functions and limiting access to information, hard copy charts, EHR, and how it is removed upon termination. Segregating access to systems based upon job title or role. Access level designations for each staff member to the facility, EHR, and paper charts.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies that explain how a user's need to know is verified before the least privileges are granted, users might be assigned greater access privileges than is needed based on the role and responsibilities. Or, you might inadvertently grant privileges to someone who has malicious intent towards the data you safekeep.

Some potential impacts include:

- Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI.
- Unauthorized disclosure (Including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
[45 CFR §164.312(a)(1)]

Develop, document, and disseminate and enforce to workforce members an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the access control policy and associated access controls.
[NIST SP 800-53 AC-1]

**T3 - §164.312(a)(1) Standard** Does your practice analyze the activities performed by all of its workforce and service providers to identify the extent to which each needs access to ePHI?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

| |
|---|
| Waverly audits all user access every 3 months, and we have the ability to see which systems, databases, or EHR are accessed at any time by anyone. Copies of our audits are maintained for 7 years. We have policies that reflect our audit activity. Access level designations for each staff member to the facility, EHR, and paper charts. |

Please include any additional notes:

| |
|---|
| Possible risk is remote access mobile access. Clinic staff can access the EHR (Practice Fusion) via a web application on their personal devices. The clinic does not manage their personal devices or require them to have antivirus software on the devices. |

Please detail your remediation plan:

| |
|---|
| |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

A "user" can be any entity that accesses your practice's ePHI, whether it is a person or a device. Consider whether your practice:

- Defines roles and responsibilities in sufficient detail to demonstrate whether access to ePHI is necessary.
- Determines whether remote access is necessary from physical environments that are not under your practice's control. If so, determine by whom, how (e.g., electronic device), and when.

*Possible Threats and Vulnerabilities:*

If your practice does not analyze activities performed by your workforce and service providers, you might not be able to identify the minimum necessary level of access necessary for ePHI.

Some potential impacts include:

- Human threats, such as a workforce member or service provider with excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.

- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the ePHI.

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
[45 CFR §164.312(a)(1)]

Analyze activities performed by all users of your information systems that create, store, and process ePHI.

Enforce role-based access control (RBAC) policies that define workforce or service providers and controls their access based upon how your practice defined user roles.
[NIST SP 800-53 AC-3]

Separate duties of workforce members and service providers with access to ePHI and define access authorizations to support those separated duties.
[NIST SP 800-53 AC-5]

Employ the principles of least privilege/minimum necessary access so your practice only enables access to ePHI for users when it is necessary to accomplish the tasks assigned to them based on their roles.
[NIST SP 800-53 AC-6]

**T4 - §164.312(a)(1) Standard** Does your practice identify the security settings for each of its information systems and electronic devices that control access?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Devices that monitor all access points within the clinic and generate reports that are reviewed by leadership to ensure only authorized staff have physical access and access to controls.

Public access to workstations. We have a courtesy workstation in our lobby for patients and visitors. We monitor all activity on this computer, and it does not have the capability of accessing any of our clinical databases, EHR, or HIPAA-sensitive databases.

Workstation access, including data access by role. We can also audit all activity for appropriate usage.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that some information systems (to include software and electronic devices) have built-in security settings for access control.

Examples of such security settings for access control include features that:

- Uniquely identify users
- Authenticate users and authentication methods
- Encrypt ePHI in transmission and storage
- Enable emergency access to ePHI

*Possible Threats and Vulnerabilities:*

If your practice does not identify the access control security settings necessary for each of its information systems and electronic devices, you are not taking full advantage of the security features available in the hardware and software.

Some potential impacts include:

- Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
[45 CFR §164.312(a) (1)]
Identify and activate access control settings for each of your information systems and electronic devices such as:

- Unique identification of individuals in group accounts (e.g., shared privilege accounts). This enables users to be held accountable for activities.
  [NIST SP 800-53 IA-2]
- Passwords, tokens, or biometrics to authenticate user identities, or some combination thereof in the case multifactor authentication.
  [NIST SP 800-53 IA-2]
- Emergency accounts granted for the short-term to allow access during an emergency.
  [NIST SP 800-53 AC-2]
- Automatic removal or deactivation of emergency accounts after the resumption of normal operations.

[NIST SP 800-53 AC-2]

**T5 - §164.312(a)(2)(i) Required** Does your practice have policies and procedures for the assignment of a unique identifier for each authorized user?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

| |
|---|
| Yes, Waverly requires 2-factor authentication (passwords) for access that is unique to each user. This policy requires that all staff change their passwords every 3 months. All PHI data is encrypted. |

Please include any additional notes:

| |
|---|
| |

Please detail your remediation plan:

| |
|---|
| |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI.
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies requiring each authorized user to have a unique identifier, your practice might not be able to keep track of authorized users and the roles and responsibilities assigned to them.

Some potential impacts include:

- An authorized user might have privileges to access more ePHI than is necessary to complete the responsibilities associated with the role filled.
- System accesses and activities undertaken cannot be attributed to a specific authorized user; therefore, your practice cannot enforce user accountability.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities.
NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Unique user identification: Assign a unique name and/or number for identifying and tracking user identity.
[45 CFR §164.312(a)(2)(i)]

Develop, document, and disseminate to workforce members an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
[NIST SP 800-53 IA-1]

**T6 - §164.312(a)(2)(i) Required** Does your practice require that each user enter a unique user identifier prior to obtaining access to ePHI?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

| |
|---|
| Yes, Waverly requires 2-factor authentication (passwords) for access that is unique to each user. This policy requires that all staff change their passwords every 3 months. All PHI data is encrypted. |

Please include any additional notes:

| |
|---|
| |

Please detail your remediation plan:

| |
|---|
| |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

○ Low

○ Medium

○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Associates authorized user privileges with each unique user identifier.
- Requires users to enter a unique identifier when accessing your practice's information systems and electronic devices; and deny access to users if the information they entered incorrect.
- Uses unique user identifier in conjunction with an authentication mechanism as part of your access control strategy.

*Possible Threats and Vulnerabilities:*

If your practice does not require a unique user identifier to be entered prior to granting access to ePHI, you might not be able to effectively limit access to ePHI based on their assigned role.

Some potential impacts include:

- Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Unique user identification: Assign a unique name and/or number for identifying and tracking user identity.
[45 CFR §164.312(a)(2)(i)]

Implement unique identification for each user prior to granting access to ePHI.
Implement unique identification of individuals in group accounts (e.g., shared privilege accounts). This will allow activities to be attributed to individuals, therefore establishing accountability for activities undertaken.
[NIST SP 800-53 IA-2]

Implement a registration process that requires supervisory authorization in order to establish an individual or group identifier. Your practice should prohibit the reuse of information systems account identifiers.
[NIST SP 800-53 IA-4]

**T7 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures to enable access to ePHI in the event of an emergency?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Waverly lists they have a policy and procedure for emergency access to PHI.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice your practice's policies do not require assurance that ePHI can be accessed in the event of an emergency in which the routine means of accessing ePHI is unavailable, then ePHI can be unavailable to enable timely and accurate diagnosis and treatment.

Some potential impacts include:

- Accurate ePHI might not be available, which can adversely impact the practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Develop, document, and disseminate to workforce members a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls;
[NIST SP 800-53 CP-1]

**T8 - §164.312(a)(2)(ii) Required** Does your practice define what constitutes an emergency and identify the various types of emergencies that are likely to occur?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Emergency incident responses and annual testing of the plan. That plan aligns with our back-up plan and emergency contingency plan. Emergency downtime plans and how to function when the EHR is not accessible. This includes disaster management, **including definitions for an emergency, staff's roles, backup procedures, and downtime procedures**. The policy identifies roles, who is responsible for activating the emergency/disaster plan. The policy also describes the frequency of disaster drills.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Clearly defines what constitutes an emergency (consistent with (consistent with Contingency Plan Standard §164.308(a)(7)(i) and the circumstances under which emergency access is enabled.

- Identifies the person capable of activating the emergency access method

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect, secure and control access to ePHI if it is unable to access ePHI during an emergency or when normal access procedures are disabled or become unavailable.

A potential impact might be that accurate ePHI is not available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.
Establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Implement role-based access control (RBAC) policies and employ audited and automated override of access control mechanisms for emergency situations.
[NIST SP 800-53 AC-3]

Implement a contingency plan that identifies essential activities and associated requirements, such as roles, responsibilities and processes for full information system restoration (e.g., termination of emergency access, reinstitution of normal access controls).
[NIST SP 800-53 CP-2]

**T9 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures for creating an exact copy of ePHI as a backup?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

| |
|---|
| Yes, Waverly has data backup to a cloud. They can access all data backed up to the cloud within 30 minutes via web access. They do not maintain backed up data on site. |

Please include any additional notes:

| |
|---|
| |

Please detail your remediation plan:

| |
|---|
| |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice's policies to not require the creation and maintenance of an exact copy of ePHI, then processes might not be in place to assure access to accurate ePHI when the ePHI source routinely accessed is unavailable, such as during an emergency. ePHI can be unavailable, thus making it difficult to provide timely and accurate diagnosis and treatment.

Some potential impacts include:

- Natural and environmental threats (e.g., fire, water, loss of power, temperature extremes) can compromise the function and integrity of your practice's information systems.
- Accurate ePHI might not be available, which can adversely impact the practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Establish an alternate storage site with the necessary agreements to permit the storage and retrieval of an exact copy of your practice's ePHI. Ensure that the alternate storage site provides information security safeguards equivalent to those of the primary site.
[NIST SP 800-53 CP-6]

Conduct backups of user-level, system- level, and security-related documentation contained in the information system. [NIST SP 800-53 CP-9]

**T10 - §164.312(a)(2)(ii) Required** Does your practice back up ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage, such as a cloud environment?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, Waverly has data backup to a cloud. They can access all data backed up to the cloud within 30 minutes via web access. They do not maintain backed up data on site.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Has the capability to back up ePHI to an off-site storage location.
- Can access the backed up ePHI and other health information in a reasonable amount of time in order to continue operations during an emergency.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to recover ePHI and other health information during an emergency or when systems become unavailable if it does not backup ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage (e.g., cloud environment).

Some potential impacts include:

- Natural and environmental threats (e.g., fire, water, loss of power, temperature extremes) can compromise the function and integrity of your practice's information systems.
- Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*

Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Establish an alternate storage site with the necessary agreements to permit the storage and retrieval of an exact copy of your practice's ePHI. Ensure that the alternate storage site provides information security safeguards equivalent to those of the primary site.
[NIST SP 800-53 CP-6]

Conduct backups of user-level, system- level, and security-related documentation contained in the information system. [NIST SP 800-53 CP-9]

**T11 - §164.312(a)(2)(ii) Required** Does your practice have **back up information systems** so that it can access ePHI in the event of an emergency or when your practice's primary systems become unavailable?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Waverly does not have redundant information systems, with the same operating system environment and real-time data replication, in order to transfer and continue operations during an emergency. **However, they do have emergency downtime plans and how to function when the EHR is not accessible.**

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

Has redundant information systems, with the same operating system environment and real-time data replication, in order to transfer and continue operations during an emergency.

*Possible Threats and Vulnerabilities:*

If your practice does not have an alternative means for accessing ePHI when its primary systems become unavailable, then your ability to continue operating your practice during an emergency can be impeded.

Some potential impacts include:

- Natural and environmental threats, such as fire, water, loss of power, and temperature extremes, can compromise the function and integrity of your practice's information systems.
- Human threats, such as an employee or service provider with unauthorized and excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.

*Examples of Safeguards:*

Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Conduct backups of user-level, system- level, and security-related documentation contained in the information system.
[NIST SP 800-53 CP-9]

**T12 - §164.312(a)(2)(ii) Required** Does your practice have the capability to **activate emergency access to its information systems** in the event of a disaster?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

| |
|---|
| Waverly states they have policies and procedures for emergency access to PHI. Unclear if this means information systems too. |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your information system to determine if its features include emergency access.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to access critical information systems and ePHI if your practice does not have the capability to activate emergency access to its information systems in the event of a disaster.

Some potential impacts include:

- Natural and environmental threats (e.g., fire, water, loss of power, temperature extremes) can compromise the function and integrity of your practice's information systems.
- Human threats, such as an employee or service provider with unauthorized and excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Implement a contingency plan that identifies roles and responsibilities for accessing ePHI and also identifies the critical information systems that are needed during an emergency.
[NIST SP 800-53 CP-2]

Enforce role-based access control (RBAC) policies that define the roles of workforce or service providers and controls access based on how your practice defined its user roles. [NIST SP 800-53 AC-3]

**T13 - §164.312(a)(2)(ii) Required** Does your practice have policies and procedures to identify the role of the individual accountable for activating emergency access settings when necessary?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Waverly does have a disaster management, including definitions for an emergency, staff's roles, backup procedures, and downtime procedures. The policy identifies roles, **who is responsible for activating the emergency/disaster plan**. The policy also describes the frequency of disaster drills.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice's policies do not require assignment of roles and responsibilities that can assure continuing access to ePHI during an emergency, then ePHI is unavailable when the routine means of access are disrupted.

Some potential impacts include:

- Human threats, such as an employee or service provider with unauthorized and excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Implement a contingency plan that identifies roles and responsibilities for accessing ePHI and also identifies the critical information systems that are needed during an emergency.
[NIST SP 800-53 CP-2]

Clearly identify the individual authorized to activate the emergency access settings.
[NIST SP 800-53 IA-2]

Enforce a role-based access control (RBAC) policy that defines the roles of the workforce or service providers and controls access based upon how your practice defined their user roles.
[NIST SP 800-53 AC-3]

**T14 - §164.312(a)(2)(ii) Required** Does your practice designate a workforce member who can activate the emergency access settings for your **information systems**?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Waverly does have a disaster management, including definitions for an emergency, staff's roles, backup procedures, and downtime procedures. The policy identifies roles, **who is responsible for activating the emergency/disaster plan**. The policy also describes the frequency of disaster drills. **Policies include emergency access to PHI.**

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Has policies and procedures in place for obtaining access to ePHI during an emergency; they should be complementary to your continuity of operations strategy.
- Identifies the person capable of activating the emergency access method.
- Assigns responsibility for implementing its emergency plans. Consider that this responsibility could be the designated workforce member for security.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to access critical information systems and ePHI during an emergency if it does not designate a workforce member who is able to access your system to activate the emergency access settings.

Some potential impacts include:

- Human threats, such as an employee or service provider with unauthorized and excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Implement a contingency plan that identifies roles and responsibilities for accessing ePHI and also identifies the critical information systems that are needed during an emergency.
[NIST SP 800-53 CP-2]

Clearly identify the individual authorized to activate the emergency access settings. [NIST SP 800-53 IA-2]

Enforce a role-based access control (RBAC) policy that defines the roles of the workforce or service providers and controls access based upon how your practice defined their user roles. [NIST SP 800-53 AC-3]

**T15 - §164.312(a)(2)(ii) Required** Does your practice test access when evaluating its ability to continue accessing ePHI and other health records during an emergency?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Waverly does have a disaster management, including definitions for an emergency, staff's roles, backup procedures, and downtime procedures. The policy identifies roles, who is responsible for activating the emergency/disaster plan. **The policy also describes the frequency of disaster drills.**

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it has methods:

- For emergency access that is automatic and auditable (documented and tested)
- For testing as part of its business continuity plan.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to provide access to critical information systems and ePHI during an emergency if your practice does not test its ability to continue accessing ePHI and other health records during an emergency.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Coordinate testing of continuity and emergency mode of operations to ensure emergency access can be activated.
[NIST SP 800-53 CP-4]

Test role-based access control (RBAC) policies to ensure that the assigned individual has the appropriate access and permissions during continuity and emergency mode of operations.
[NIST SP 800-53 AC-3]

**T16 - §164.312(a)(2)(ii) Required** Does your practice effectively recover from an emergency and resume normal operations and access to ePHI?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Evaluate your practice to determine if it clearly explains when and how to reinstitute normal access controls once an emergency passes. This might be part of your business continuity strategy. Your practice might not be able to reinstitute normal access controls after an emergency if your practice does not clearly explain when and how to recover from an emergency.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it clearly explains when and how to reinstitute normal access controls once an emergency passes. This might be part of your business continuity strategy.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to reinstitute normal access controls after an emergency if your practice does not clearly explain when and how to recover from an emergency.

Some potential impacts include:

- Human threats, such as an employee with unauthorized and excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.
- Accurate ePHI is not available, adversely impacting a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
[45 CFR §164.312(a)(2)(ii)]

Implement a contingency plan that identifies essential activities and associated requirements (e.g., roles, responsibilities and processes for full information system restoration). This would include the termination of emergency access and the reinstitution of normal access controls.
[NIST SP 800-53 CP-2]

Implement a restoration capability for information systems components within a predetermined time period to a known operational state.
[NIST SP 800-53 CP-10]

**T17 - §164.312(a)(2)(iii) Addressable** Does your practice have policies and procedures that require an authorized user's session to be automatically logged-off after a predetermined period of inactivity?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, Waverly has policies and procedures that include a staff's user session will log them out if there is no activity (EHR, clinical data bases etc.) in 5 minutes of non-activity.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

○ Low

○ Medium

○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

○ Low

○ Medium

○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice's policies and procedure do not require that its information systems automatically log-off after a user is inactive on the system for a specified period of time, a user's session can remain accessible when a workstation is unattended.

Some potential impacts include:

- Unauthorized users can access ePHI and the activities undertaken by the unauthorized user will be attributed to the user who abandon the open session.

- Human threats, such as personnel with unauthorized access, can compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
[45 CFR §164.312(a)(2)(iii)]

Develop, document, and disseminate to workforce members an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
[NIST SP 800-53 IA-1]

Enforce an automated session lock after a predetermined period of inactivity or upon receiving a request from a user. Retain the session lock until the user reestablishes access using the established identification and authentication procedures.
[NIST SP 800-53 AC-11 and AC-12]

**T18 - §164.312(a)(2)(iii) Addressable** Does a responsible person in your practice know the automatic logoff settings for its information systems and electronic devices?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Identify information system components and **responsible person in your practice** who oversees electronic devices with auto log-off capabilities.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Logoff refers to a user logging off of the system.

Information system refers to an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Electronic devices include nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Many software applications and devices are able to engage a screen lock or terminate a session when the user is inactive for a period of time. This capability is designed to limit access to the device or software and the ePHI can be recalled, modified, transmitted, and stored.

Evaluate your practice to determine if its information systems and electronic devices have an automatic log off function and how it can be activated.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect, secure and control access to its ePHI if it does not enforce automatic logoff procedures that terminate an electronic session after a predetermined period of inactivity.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
[45 CFR §164.312(a)(2)(iii)]

Identify information system components and electronic devices with auto log-off capabilities.
[NIST SP 800-53 CM-8]

Enforce an automated session lock after a predetermined period of inactivity or upon receiving a request from a user. Retain the session lock until the user reestablishes access using the established identification and authentication procedures.
[NIST SP 800-53 AC-11 and AC-12]

**T19 - §164.312(a)(2)(ii) Addressable** Does your practice activate an automatic logoff that terminates an electronic session after a predetermined period of user inactivity?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

| |
|---|
| Yes, Waverly has policies and procedures that include a staff's user session will automatically log them out if there is no activity (EHR, clinical data bases etc.) in 5 minutes of non-activity. |

Please include any additional notes:

| |
|---|
| |

Please detail your remediation plan:

| |
|---|
| |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice's information systems to determine if it:

- Logs off by automatically terminating an electronic session after a period of user inactivity and remains logged off until the user reestablishes access.
- Enforces the period of user inactivity that triggers the automatic logoff.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect, secure and control access to its ePHI if it does not enforce automatic logoff procedures that terminate an electronic session after a predetermined period of inactivity.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
[45 CFR §164.312(a)(2)(iii)]

Identify an inventory of information system components and electronic devices with auto log-off capabilities.
[NIST SP 800-53 CM-8]

Enforce an automated session lock after a predetermined period of inactivity or upon receiving a request from a user. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
[NIST SP 800-53 AC-11] and [NIST SP 800-53 AC-12]

**T20 - §164.312(a)(2)(iv) Addressable** Does your practice have policies and procedures for implementing mechanisms that can encrypt and decrypt ePHI?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Yes, Waverly ensures all computer workstations, including exam room PCs, are **encrypted** and require staff to log in and out. There is a privacy screen on all workstation monitors. All PHI data is encrypted.

Please include any additional notes:

Risk: Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies regarding mechanisms that can encrypt and decrypt ePHI, then encryption is not considered among safeguards available for protecting ePHI. Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement a mechanism to encrypt and decrypt ePHI.
[45 CFR §164.312(a)(2)(iv)]

Develop, document, and disseminate to workforce members a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
[NIST SP 800-53 SC-1]

**T21 - §164.312(a)(2)(iv) Addressable** Does your practice know the encryption capabilities of its information systems and electronic devices?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Risk: Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please include any additional notes:

Please detail your remediation plan:

| |
|---|
| Waverly is looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted. Evaluate your practice to determine if is inventory of its information systems indicates whether it has encryption capabilities. Information systems include software, applications, hardware, and electronic devices. |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Some information systems and electronic devices have encryption capabilities built in, while others are capable of working with off-the-shelf encryption software.

Portable electronic devices are non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes, but is not limited to, laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Evaluate your practice to determine if is inventory of its information systems indicates whether it has encryption capabilities. Information systems include software, applications, hardware, and electronic devices.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to use encryption and decryption mechanisms to protect, secure, and control access to its ePHI if it does not know the encryption and decryption capabilities of its information systems and electronic devices

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement a mechanism to encrypt and decrypt ePHI.
[45 CFR §164.312(a)(2)(iv)]

Identify an inventory of information system components and electronic devices with data encryption capabilities.
[NIST SP 800-53 CM-8]

Assess and measure the risk of information being either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception.
[NIST SP 800-53 SC-8]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission unless otherwise protected by physical security

controls.
[NIST SP 800-53 SC-13]

**T22 - §164.312(a)(2)(iv) Addressable** Does your practice control access to ePHI and other health information by using encryption/decryption methods to deny access to unauthorized users?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Workstation access, including data access by role. We can also audit all activity for appropriate usage. Unclear whether or not if access is denied to unauthorized users.

Please include any additional notes:

Please detail your remediation plan:

| |
|---|
| Waverly should implement encryption controls to reduce the risk for unauthorized access to ePHI and other health information when it is stored/maintained on an electronic device or portable media that is at greater risk of loss or theft (such as laptop, tablet, smartphone, or thumb device). Ensures that encryption standards are consistent with leading practices. |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Should implement encryption controls to reduce the risk for unauthorized access to ePHI and other health information when it is stored/maintained on an electronic device or portable media that is at greater risk of loss or theft (such as laptop, tablet, smartphone, or thumb device).
- Ensures that encryption standards are consistent with leading practices.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to ensure access to its ePHI is denied to unauthorized users if it does not use encryption/decryption methods to control access to ePHI and other health information.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement a mechanism to encrypt and decrypt ePHI.
[45 CFR §164.312(a)(2)(iv)]

Enforce role-based access control (RBAC) policies that define workforce or service providers and controls access based upon how your practice defined their user roles.
[NIST SP 800-53 AC-3]

Identify an inventory of information system components and electronic devices with data encryption capabilities that accurately reflects the current information system environment.
[NIST SP 800-53 CM-8]

Assess and measure the risk of information being either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception.
[NIST SP 800-53 SC-8]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI while also detecting changes to information during transmission (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]

**T23 - §164.312(b) Standard** Does your practice have policies and procedures identifying hardware, software, or procedural mechanisms that record or examine information systems activities?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, Waverly can audit all activity for appropriate usage.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies regarding mechanisms (hardware and software) that can record and examine information system activity, then inappropriate use of information systems and access of ePHI can go undetected.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Develop, document, and disseminate to workforce members an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
[NIST SP 800-53 AU-1]

Identify and periodically review and update key audit events (e.g., activities that create, store, and transmit ePHI) and those that are significant to the security of information systems and the environments in which they operate in order to support ongoing audit needs.
[NIST SP 800-53 AU-2]

**T24 - §164.312(b) Standard** Does your practice identify its activities that create, store, and transmit ePHI and the information systems that support these business processes?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Your practice might not implement access controls to protect its ePHI if it does not identify the activities that create, store, and transmit ePHI and the information systems that support these activities. Recommend identifying such activities and systems that support them.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Activities refer to the tasks that your practice's workforce members and service providers perform that involve the collection, use, transmission, and storage of ePHI.

*Possible Threats and Vulnerabilities:*

Your practice might not implement access controls to protect its ePHI if it does not identify the activities that create, store, and transmit ePHI and the information systems that support these activities.

Some potential impacts include:

- Human threats, such as an employee or service provider with excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Identify and periodically review and update key audit events (e.g., activities that create, store, and transmit ePHI) and those that are significant to the security of information systems and the environments in which they operate in order to support ongoing audit needs.
[NIST SP 800-53 AU-2]

**T25 - §164.312(b) Standard** Does your practice categorize its activities and information systems that create, transmit or store ePHI as high, moderate or low risk based on its risk analyses?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Identify and categorize key audit events (e.g., those that create, store, and transmit ePHI) as high, medium or low risk. Identify those that are significant to the security of information systems and the environments in which those operate in order to meet specific ongoing audit needs.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider categorizing your practice's risks as high, moderate or low based on the risk analysis you have completed.

Consider that ePHI-related activities are often a target of human threats. When these activities are supported by information systems and electronic devices with known vulnerabilities, your practice's ePHI can be at a high risk of being compromised.

*Possible Threats and Vulnerabilities:*

Your practice might not be able identify high and low risk business processes if it does not categorize activities and information systems that create, transmit, or store ePHI (as high, moderate or low risk based on its risk analyses).

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Document and disseminate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, compliance, procedures, and the coordination necessary among organizational entities to implement the audit.
[NIST SP 800-53 AU-1]

Identify and categorize key audit events (e.g., those that create, store, and transmit ePHI) as high, medium or low risk. Identify those that are significant to the security of information systems and the environments in which those operate in order to meet specific ongoing audit needs.
[NIST SP 800-53 AU-2]

**T26 - §164.312(b) Standard** Does your practice use the evaluation from its risk analysis to help determine the frequency and scope of its audits, when identifying the activities that will be tracked?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Audits are done every 6 months.

Please include any additional notes:

Please detail your remediation plan:

| |
|---|
| Use the risk-based categorization of key audit events (e.g., activities that create, store, and transmit ePHI) in order to determine the scope and frequency of audits. |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Coordinates the security audit function with other parts of its operations that require audit-related information to enhance mutual support and to help with the selection of auditable events.

- Uses system categorization to identify high-risk systems requiring greater attention.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to identify which business activities are at highest risk, and subsequently determine the appropriate frequency and scope of its audits, if it does not use the results of its previous risk analyses.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Document and disseminate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, compliance, procedures, and the coordination that is necessary among key stakeholders to implement the audit.
[NIST SP 800-53 AU-1]

Use the risk based categorization of key audit events (e.g., activities that create, store, and transmit ePHI) in order to determine the scope and frequency of audits.
[NIST SP 800-53 AU-2]

**T27 - §164.312(b) Standard** Does your practice have audit control mechanisms that can monitor, record and/or examine information system activity?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Waverly audits all user access every 3 months, and we have the ability to see which systems, databases, or EHR are accessed at any time by anyone. Copies of our audits are maintained for 7 years. We have policies that reflect our audit activity.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Some information systems and electronic devices have built-in audit capabilities. Activating such features enables your practice to have a ready way to monitor information system activity and discover misuse. Other audit control mechanisms might need to be acquired.

Auditing tools can be third-party products, freeware, firmware, or tools that your practice might build itself. Understanding current information system capabilities enables your practice to make the best use of the resources that are available before seeking out additional tools that are available in the marketplace.

Records (e.g., access/audit logs), firewall system activity, and similar documentation exist to serve purposes of monitoring and auditing.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to detect, prevent, and document unauthorized system activity if its information systems do not have audit control mechanisms that can monitor, record and/or examine information system activity.

Some potential impacts include:

- Human threats, such as an employee or service provider with excessive or unauthorized access privileges, can go undetected and your practice might not be able to prevent a potential compromise to ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Configure information systems and components to automatically capture and generate audit records containing information that establishes what type of event occurred, when and where it occurred, its source, and the outcome. You should also collect information on the identity of any individuals or subjects associated with the event.
[NIST SP 800-53 AU-3]

Periodically review and analyze your information system's audit records for indications of inappropriate or unusual activity.
[NIST SP 800-53 AU-6]

Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and does not alter the original content or time ordering of audit records.
[NIST SP 800-53 AU-7]

**T28 - §164.312(b) Standard** Does your practice have policies and procedures for creating, retaining, and distributing audit reports to appropriate workforce members for review?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Copies of our audits are maintained for 7 years. We have policies that reflect our audit activity. Creating, approving and managing audit policies. That policy indicates we keep all audit polices for at least 6 years, but we actually keep them 7 years to be consistent with our medical records. All of our audits are reviewed by leadership and shared with staff to assist in understanding threats and vulnerabilities. We audit access controls to software, hardware and physical buildings every 6 months.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI.
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies and procedures for distributing reports about information system activity and access to ePHI, then those accountable for enforcing appropriate use of information and information technology can be unable to perform the responsibilities associated with their role.

Some potential impacts include:
Unauthorized and inappropriate system activity and ePHI access can go undetected.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Develop, document, and disseminate to workforce members an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
[NIST SP 800-53 AU-1]

**T29 - §164.312(b) Standard** Does your practice generate the audit reports and distribute them to the appropriate people for review?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Copies of our audits are maintained for 7 years. We have policies that reflect our audit activity. Creating, approving and managing audit policies. That policy indicates we keep all audit polices for at least 6 years, but we actually keep them 7 years to be consistent with our medical records. All of our audits are reviewed by leadership and shared with staff to assist in understanding threats and vulnerabilities. We audit access controls to software, hardware and physical buildings every 6 months.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that your practice can only derive value from its audit and logging documentation when it reviews reports.
Consider that sharing information with the person accountable for the secure operation of an information system enables them to identify unauthorized access and inappropriate access, while also helping your practice respond in accordance with its security plan.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to detect, prevent, and document unauthorized system activity if it does not generate audit reports and distribute them to the appropriate people for review.

Some potential impacts include:

- Human threats, such as an employee or service provider with excessive or unauthorized access privileges, can go undetected and your practice might not be able to prevent a potential compromise to ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Document and disseminate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, compliance, procedures, and the coordination necessary among organizational entities to implement the audit.
[NIST SP 800-53 AU-1]

Periodically review and analyze your information system's audit records for indications of inappropriate or unusual activity.
[NIST SP 800-53 AU-6]

Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and does not alter the original content or time ordering of audit records.
[NIST SP 800-53 AU-7]

**T30 - §164.312(b) Standard** Does your practice have policies and procedures establishing retention requirements for audit purposes?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Copies of our audits are **maintained for 7 years.** We have policies that reflect our audit activity. Creating, approving and managing audit policies. That policy indicates we keep all audit polices for at least 6 years, but we actually keep them 7 years to be consistent with our medical records.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies that specify how and for how long audit/access records are retained, then audit/access records can be unavailable when they are needed to facilitate or support an investigation.

Some potential impacts include:

- Unauthorized and inappropriate system activity and ePHI access can go undetected.

Users might not be held accountable for unauthorized system activity.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Develop, document, and disseminate to workforce members an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
[NIST SP 800-53 AU-1]

**T31 - §164.312(b) Standard** Does your practice retain copies of its audit/access records?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Copies of audits are **maintained for 7 years.** We have policies that reflect our audit activity. Creating, approving and managing audit policies. That policy indicates we keep all audit polices for at least 6 years, but we actually keep them 7 years to be consistent with our medical records.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that the generation of access/audit reports necessitates storage. To have value, the reports must be available for review.

Consider that your practice can only derive value from its audit and logging documentation when it reviews reports.

*Possible Threats and Vulnerabilities:*

If your practice does not retain copies of its audit records, it might not be able to include this information in a review of auditable events

Violations of acceptable use policies and procedures go unobserved.

- Human threats, such as an employee or service provider with excessive or unauthorized access privileges, can go undetected and your practice might not be able to prevent a potential compromise to ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Consider the types of audit and the audit processing requirements when allocating audit storage capacity. Configure your information system so that it periodically transfers audit records to an alternate system or media in order to utilize storage capacity effectively.
[NIST SP 800-53 AU-4]

Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and does not alter the original content or time ordering of audit records.

**T31 - §164.312(b) Standard** Does your practice retain copies of its audit/access records?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Copies of audits are **maintained for 7 years.** We have policies that reflect our audit activity. Creating, approving and managing audit policies. That policy indicates we keep all audit polices for at least 6 years, but we actually keep them 7 years to be consistent with our medical records.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that the generation of access/audit reports necessitates storage. To have value, the reports must be available for review.

Consider that your practice can only derive value from its audit and logging documentation when it reviews reports.

*Possible Threats and Vulnerabilities:*

If your practice does not retain copies of its audit records, it might not be able to include this information in a review of auditable events

Violations of acceptable use policies and procedures go unobserved.

- Human threats, such as an employee or service provider with excessive or unauthorized access privileges, can go undetected and your practice might not be able to prevent a potential compromise to ePHI.

- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
[45 CFR §164.312(b)]

Consider the types of audit and the audit processing requirements when allocating audit storage capacity. Configure your information system so that it periodically transfers audit records to an alternate system or media in order to utilize storage capacity effectively.
[NIST SP 800-53 AU-4]

Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and does not alter the original content or time ordering of audit records.

**T32 - §164.312(c)(1) Standard** Does your practice have policies and procedures for protecting ePHI from unauthorized modification or destruction?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice's policies and procedures identify circumstances in which appropriate approval is required prior to altering, modifying or destroying ePHI.

Does the risk analysis performed by your practice identify what data must be authenticated to corroborate that e-PHI has not been improperly altered or destroyed?

*Possible Threats and Vulnerabilities:*

Your practice may not be able to safeguard its ePHI if it does not have policies and procedures for protecting ePHI from unauthorized modification or destruction.

Some potential impacts include:

- Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI.
- Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
- Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
[45 CFR §164.312(c)(1)]

Develop, document, and disseminate to workforce members an information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the information integrity policy and associated information integrity controls.
[NIST SP 800-53 SI-1]

**T33 - §164.312(c)(2) Addressable** Does your practice have mechanisms to corroborate that ePHI has not been altered, modified or destroyed in an unauthorized manner?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Waverly is looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please include any additional notes:

Please detail your remediation plan:

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice has data authentication mechanisms and tools, such as checksum. Checksum is a computation that is introduced when ePHI is transmitted or stored. The computation is checked at a later time (such as when ePHI recalled or when it is received at the intended destination) to ascertain whether the computations match. If the checksum matches, then it is less likely that the ePHI was altered or modified. Also consider whether your practice relies on encryption validation to authenticate ePHI.

*Possible Threats and Vulnerabilities:*

Your practice may not be able to safeguard its ePHI if it does not have authentication mechanisms and tools, such as data encryption validation, that can authenticate ePHI.

Some potential impacts include:

- Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI.
- Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
- Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
[45 CFR §164.312(C)(2)]

Employ integrity verification tools to detect unauthorized changes to ePHI and provide notifications to management upon discovering discrepancies during integrity verification.
[NIST SP 800-53 SI-7]

**T34 - §164.312(d) Required** Does your practice have policies and procedures for verification of a person or entity seeking access to ePHI is the one claimed?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Waverly has policies and procedures requiring 2-factor authentication (passwords) for access that is **unique to each user**. This policy requires that all staff change their passwords every 3 months. All PHI data is encrypted.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not authenticate (verify the uniquely identified user is the one claimed), then unauthorized users can access your practice's information systems and ePHI.

Some potential impacts include:

- Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI.

Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
[45 CFR §164.312(d)]

Develop, document, and disseminate to workforce members an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
[NIST SP 800-53 IA-1]

**T35 - §164.312(d) Required** Does your practice know the authentication capabilities of its information systems and electronic devices to assure that a uniquely identified user is the one claimed?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. Implement unique identification of individuals in group accounts (e.g., shared privilege accounts). This facilitates detailed accountability of individual activities. Identify the various authentication capabilities of the information systems and components such as passwords, tokens, biometrics or some combination thereof.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

When evaluating your practice, consider that authentication requires establishing the validity of a transmission source, whether the source is an individual or an entity, such as another electronic device or information system.

Evaluate your practice to determine the authentication methods and mechanisms that it uses, such as passwords, smart cards, digital certificates, and biometrics.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to assure that a uniquely identified user is the one claimed if your practice does not understand the authentication capabilities of its information systems and electronic devices.

Some potential impacts include:

- Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
[45 CFR §164.312(d)]

Implement unique identification of individuals in group accounts (e.g., shared privilege accounts). This facilitates detailed accountability of individual activities.
[NIST SP 800-53 IA-2]

Identify the various authentication capabilities of the information systems and components such as passwords, tokens, biometrics or some combination thereof.
[NIST SP 800-53 IA-2]

**T36 - §164.312(d) Required** Does your practice use the evaluation from its risk analysis to select the appropriate authentication mechanism?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Evaluate your practice to determine if it:

- Knows the advantages and disadvantages of each authentication method.
- Determines the suitability of each authentication method based on its analysis of risks
- Ensures that similar information systems with a similar level of risk implement the same authentication methods

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Knows the advantages and disadvantages of each authentication method.
- Determines the suitability of each authentication method based on its analysis of risks
- Ensures that similar information systems with a similar level of risk implement the same authentication methods

Also, as you perform the evaluation, you may consult NIST publications that have information on leading industry practices and methods.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to determine and implement a suitable authentication method for your practice if it does not use the results of its risk analyses to select the appropriate authentication mechanism.

Some potential impacts include:

- Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
[45 CFR §164.312(d)]

Implement unique identification for individuals in group accounts (e.g., shared privilege accounts). This will facilitate detailed accountability of individual activities.
[NIST SP 800-53 IA-2]

Identify the various authentication capabilities of your information systems and components such as passwords, tokens, biometrics or some combination thereof.
[NIST SP 800-53 IA-2]

Conduct risk assessments to determine authentication requirements and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to ePHI and having information systems with a need to protect and adequately mitigate risk.
[NIST SP 800-53 IA-8]

**T37 - §164.312(d) Required** Does your practice protect the confidentiality of the documentation containing access control records (list of authorized users and passwords)?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Protect the confidentiality of the documentation containing access control records (list of authorized users and passwords).

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Has access control that ensures the integrity of databases that store unique user identifiers and authenticators, such as passwords.

Uses encrypting passwords and other authentication information to help reduce the risk that unauthorized users can access password files and compromise access controls already in place.

*Possible Threats and Vulnerabilities:*

If your practice does not protect the confidentiality of the documentation containing access control records, your practice might not be able to secure access to your database(s) containing password files, which might compromise the access controls in place.

Some potential impacts include:

- Human threats, such as an employee or service provider with excessive or unauthorized access privileges, can go undetected and your practice might not be able to prevent a potential compromise to ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
[45 CFR §164.312(d)]

Implement unique identifiers for individuals in group accounts (e.g., shared privilege accounts). This will facilitate detailed accountability of individual activities.
[NIST SP 800-53 IA-2]

Identify the various authentication capabilities of the information systems and components such as passwords, tokens, biometrics or some combination thereof.
[NIST SP 800-53 IA-2]

Enforce role-based access control (RBAC) policies that define workforce or service providers and controls access based upon how your practice defined users' roles.
[NIST SP 800-53 AC-3]

Employ the principles of least privilege/minimum necessary access so your practice only enables access to ePHI for workforce members and service providers when it is necessary to accomplish the tasks assigned to them based on their individual roles.
[NIST SP 800-53 AC-6]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission and storage (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]

**T38 - §164.312(e)(1) Standard** Does your practice have policies and procedures for guarding against unauthorized access of ePHI when it is transmitted on an electronic network?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider having written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice does not have policies and procedures designed to guard against unauthorized access of ePHI when it is being transmitted via a communication network, then ePHI can be intercepted by unauthorized users.

*Examples of Safeguards:*

Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communication network.
[45 CFR §164.312(e)(1)]

Develop, document, and disseminate to workforce members a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
[NIST SP 800-53 SC-1]

**T39 - §164.312(e)(1) Standard** Do your practice implement safeguards, to assure that ePHI is not accessed while en-route to its intended recipient?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice assures that the safeguards it implements are consistent with those in similar practices that are compliant with the HIPAA Security Rule.

*Possible Threats and Vulnerabilities:*

Your ePHI might be accessed and compromised while en-route to its intended recipient if your practice does not implement leading practices to protect ePHI when it is transmitted.

Some potential impacts include:

- Unauthorized access can go undetected and your practice might not be able to reduce the risk to the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

Accurate ePHI is not available, adversely impacting a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communication network.
[45 CFR §164.312(e)(1)]

Assess and measure the risk of information being either unintentionally or maliciously accessed or modified during preparation for transmission or during reception.
[NIST SP 800-53 SC-8]

Implement encryption to prevent unauthorized disclosure of ePHI and detect changes to information during transmission (unless otherwise protected by physical security controls). [NIST SP 800-53 SC-13]

**T40 - §164.312(e)(2)(i) Addressable** Does your practice know what encryption capabilities are available to it for encrypting ePHI being transmitted from one point to another?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

| |
|---|
| Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted. |

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Knows whether or not its information systems and electronic devices are capable of encrypting transmissions
- Knows whether or not encryption technology can be acquired to work with your information systems and electronic devices.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to use the most suitable encryption and decryption mechanisms to protect, secure and control access to its ePHI if it does not know the types of encryption and decryption capabilities available in your information systems and electronic devices.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until it is disposed.
[45 CFR §164.312(e)(2)(i)]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]

Assess and measure the risk of information being unintentionally or maliciously disclosed or modified during preparation for transmission or during reception.
[NIST SP 800-53 SC-8]

**T41 - §164.312(e)(2)(i) Addressable** Does your practice take steps to reduce the risk that ePHI can be intercepted or modified when it is being sent electronically?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Waverly is currently working on this. Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate your practice to determine if it:

- Includes encryption among its options for mechanisms that protect ePHI and other health information being transmitted from one point to another
- Understands the risks associated with relying on wireless technology to transmit ePHI within the office.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect, secure, and control access to its ePHI if it does not take steps to reduce the risk of that information being intercepted or modified when it is sent electronically.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*

Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until it is disposed.
[45 CFR §164.312(e)(2)(i)]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI, while also detecting changes to information during transmission (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]

**T42 - §164.312(e)(2)(i) Addressable** Does your practice implement encryption as the safeguard to assure that ePHI is not compromised when being transmitted from one point to another?

○ Yes

○ No

**If no**, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

○ Low

○ Medium

○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that encryption protects ePHI and other health information from unauthorized access, modification, and destruction when it is being transmitted from one point to another. This includes transmission within your office or between your practice and another entity.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect and secure the integrity and confidentiality of ePHI if it does not implement encryption to ensure that ePHI is not compromised during transmission from one point to another.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until it is disposed.
[45 CFR §164.312(e)(2)(i)]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI and detect changes to information during transmission (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]

**T44 - §164.312(e)(2)(ii) Addressable** Does your practice have policies and procedures for encrypting ePHI when deemed reasonable and appropriate?

- ○ Yes
- ○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

All PHI is encrypted.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that written policies and procedures that:

- Can drive the development of processes and adoption of standards and controls, which reduce risk to ePHI
- Can provide essential information for privacy and security awareness and role-based training.

*Possible Threats and Vulnerabilities:*

If your practice's polices do not require ePHI to be encrypted when it is appropriate to do so, then it is not required to consider all appropriate means available to protect the confidentiality, integrity, and availability of ePHI when it is stored and transmitted.

Some potential impacts include:

- Unauthorized access can go undetected and your practice might not be able to reduce the risk to the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.
- Accurate ePHI is not available, adversely impacting the practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement a mechanism to encrypt ePHI whenever deemed appropriate.
[45 CFR §164.312(e)(2)(ii)]

Develop, document, and disseminate to workforce members a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
[NIST SP 800-53 SC-1]

**T45 - §164.312(e)(2)(ii) Addressable** When analyzing risk, does your practice consider the value of encryption for assuring the integrity of ePHI is not accessed or modified when it is stored or transmitted?

○ Yes

○ No

**If no**, please select from the following:

- ○ Cost
- ○ Practice Size
- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Yes, that is why we are considering human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI. As stated, we are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted.

Please include any additional notes:

Please detail your remediation plan:

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

Please rate the impact of a threat/vulnerability affecting your ePHI:

- ○ Low
- ○ Medium
- ○ High

**Overall Security Risk:**

- ○ Low
- ○ Medium
- ○ High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Evaluate actual costs, ease of implementing, and effectiveness of encryption technology for your practice.

*Possible Threats and Vulnerabilities:*

Your practice might not be able to protect and secure the integrity and confidentiality of ePHI if it does not analyze the risk and value of using encryption where appropriate.

Some potential impacts include:

- Human threats, such as personnel with unauthorized access, can intercept and compromise the privacy, confidentiality, integrity or availability of ePHI.
- Unauthorized disclosure (including disclosure through theft and loss) of ePHI can lead to identity theft.

- Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient.

*Examples of Safeguards:*
Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement a mechanism to encrypt ePHI whenever deemed appropriate.
[45 CFR §164.312(e)(2)(ii)]

Implement cryptographic mechanisms to prevent unauthorized disclosure of ePHI, while also detecting changes to information during transmission (unless otherwise protected by physical security controls).
[NIST SP 800-53 SC-13]