Combined courtesy of KHIT.org

The Office of the National Coordinator for
Health Information Technology

Physical Safeguards, pg. 193

Technical Safeguards, pg. 333

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
Administrative Safeguards Content

Version Date: March 2014

Total 436 pages:

Administrative, 192

Physical, 104

Technical, 140

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 and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

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
ONC	The Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
RBAC	Role-based Access Control
SRA	Security Risk Assessment
SRA Tool	Security Risk Assessment Tool
USB	Universal Serial Bus

A1 - §164.308(a)(1)(i) Standard Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its Electronic Protected Health Information (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:

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

Related Information:

Things to Consider to Help Answer the Question:

An information system is 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 users.

A portable electronic device is any 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.

Electronic storage media includes memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

Consider whether your practice has an inventory that includes:

- All information systems (including the components, hardware, and software that comprise them).
- All electronic devices (including laptops, tablets, and smart phones).
- All mobile media (such as thumb drives, mobile hard drives, and magnetic media).

Consider whether your practice identifies all spreadsheets, databases and other software programs that collect, process, and store ePHI.

Possible Threats and Vulnerabilities:

Your practice may not have adequate controls to safeguard ePHI if it does not develop and implement policies and procedures for assessing and managing risk to its 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 prevent, detect, contain, and correct security violations. [45 CFR §164.308(a)(1)(i)]

Develop, document, and disseminate to workforce members a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls. [NIST SP 800-53 RA-1]

A2 - §164.308(a)(1)(i) Standard Does your practice have a process for periodically reviewing its risk analysis policies and procedures and making updates as necessary?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

You should consider that technology, vulnerabilities, and threats evolve and change over time. Your practice's risk analysis policies and procedures need to adapt to meet its changing needs.

Possible Threats and Vulnerabilities:

Your practice may not be able to update and improve its safeguards for protecting ePHI if it does not periodically review its risk assessment policies and procedures,

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 prevent, detect, contain, and correct security violations.
[45 CFR §164.308(a)(1)(i)]

Review and update the current risk assessment policy and procedures to adapt your security program to changing needs.
[NIST SP 800-53 RA-1]

A3 - §164.308(a)(1)(ii)(A) Required Does your practice categorize its information systems based on the potential impact to your practice should they 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:

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

Related Information:

Things to Consider to Help Answer the Question:

***Risk analys*is** is the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Parts of risk management are synonymous with risk assessment.

Consider whether your practice categorizes its information systems as high, moderate or low impact systems.

Consider that information system categorization helps your practice to scope audits and prioritize investments for security mitigation.

Consider whether your practice's risk analysis is designed to protect its information systems and ePHI that it processes, stores, and transmits from unauthorized access, use, disclosure, disruption, change, or damage.

Consider whether your practice's risk analysis:

- Identifies threats
- Identifies vulnerabilities inherent in its technology, processes, workforce, and vendors
- Contemplates the likelihood of occurrence
- Estimates the potential magnitude of harm

Possible Threats and Vulnerabilities:

You may not be able to identify which information systems and applications are most critical to your practice's operations if they are not categorized based on the potential impacts to your practice should they become unavailable.

This failure to categorize your information systems could impact your practice in that timely and accurate ePHI may not be available, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

Examples of Safeguards:

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

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
[45 CFR §164.308(a)(1)(ii)(A)]

Categorize information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.
[NIST SP 800-53 RA-2]

Document the security categorization results (including supporting rationale) in the security plan for the information system.
[NIST SP 800-53 RA-2]

Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.
[NIST SP 800-53 RA-2]

A4 - §164.308(a)(1)(ii)(A) Required Does your practice periodically complete an accurate and thorough risk analysis, such as upon occurrence of a significant event or change in your business organization or environment?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that a significant event might be:

- A security incident
- Notification by Community Emergency Response Team (CERT) or other authority of a weakness and a threat that might act upon it
- Information about risk received from a whistleblower

Possible Threats and Vulnerabilities:

Your practice may not be able to proactively implement safeguards that address changes in risk to ePHI if it does not periodically complete an accurate and thorough risk analysis, such as upon occurrence of a significant event or change in your business organization or environment.

A failure to periodically update your risk analysis could impact your practice in that timely and accurate ePHI may not be available, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

Examples of Safeguards:

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

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
[45 CFR §164.308(a)(1)(ii)(A)]

Conduct an assessment of risk (e.g., the likelihood and magnitude of harm) from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
[NIST SP 800-53 RA-3]

A5 - §164.308(a)(1)(ii)(B) Required Does your practice have a formal documented program to mitigate the threats and vulnerabilities to ePHI identified through the risk analysis?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has a documented method for managing risk that relies on the findings included in its risk assessment to identify the appropriate management and operational or technical safeguards to manage risk to an acceptable level.

Possible Threats and Vulnerabilities:

Your practice may not be able to implement effective safeguards to manage risks to ePHI if it does not have a formal, documented program to mitigate threats and vulnerabilities identified as a result of conducting a risk analysis.

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 might not be available, which can adversely impact your healthcare professionals' ability to diagnose and treat the patient.

Examples of Safeguards:

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).
[45 CFR §164.308(a)(1)(ii)(B)]

Document within a security plan the controls and methods in place or planned to mitigate the threats and vulnerabilities to ePHI identified as a result of conducting a risk analysis.
[NIST SP 800-53 PL-2]

A6 - §164.308(a)(1)(ii)(B) Required Does your practice assure that its risk management program prevents against the impermissible use and disclosure of 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that the HIPAA privacy Rule establishes national standards by allowing ePHI to be used or disclosed only when permitted or required.

Possible Threats and Vulnerabilities:

Your practice may not be able protect and secure ePHI if it does not assure that its risk management program prevents against the impermissible use and disclosure of 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 timely available, which can adversely impact your healthcare professionals' ability to diagnose and treat their patient.

Examples of Safeguards:

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).
[45 CFR §164.308(a)(1)(ii)(B)]

Have a security plan that documents security safeguards and methods in place or planned to mitigate the threats and vulnerabilities to ePHI that are identified as a result of conducting a risk analysis.
[NIST SP 800-53 PL-2]

A7 - §164.308(a)(1)(ii)(B) Required Does your practice document the results of its risk analysis and assure the results are distributed to appropriate members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified through the risk analysis?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice documents:

- Its current and planned security controls in a security plan
- A plan of action with milestones for implementing safeguards.

Possible Threats and Vulnerabilities:

Your practice may not be able to implement effective safeguards to protect ePHI if it does not document and share the results of your risk analysis with the staff responsible for making risk management decisions, developing risk-related policies, and implementing risk mitigation safeguards for 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).
[45 CFR §164.308(a)(1)(ii)(B)]

Document, review, and disseminate risk assessment results to members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified as a result of a risk assessment.
[NIST SP 800-53 RA-3]

A8 - §164.308(a)(1)(ii)(B) Required Does your practice formally document a security plan?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Security controls (or security measures) include all of the administrative, physical, and technical safeguards in an information system.

Consider that a security plan addresses the confidentiality, integrity, and availability of your ePHI and includes strategies for a:

- Continuity Plan
- Emergency Access Plan
- Disaster Recovery Plan
- Vendor Management Plan

Possible Threats and Vulnerabilities:

Your practice may not be able to implement effective safeguards to protect ePHI if it does not formally document a security plan, which includes administrative, physical, and technical safeguards.

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).
[45 CFR §164.308(a)(1)(ii)(B)]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should

also outline procedures to facilitate its implementation of the security planning policy and associated controls.
[NIST SP 800-53 PL-1]

A9 - §164.308(a)(1)(ii)(C) Required Does your practice have a formal and documented process or regular human resources policy to discipline workforce members who have access to your organization's ePHI if they are found to have violated the office's policies to prevent system misuse, abuse, and any harmful activities that involve your practice's 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that policies and procedures must be enforced in order to be effective.

Consider whether your practice consulted legal counsel in the drafting of its workforce sanctions policy.

Consider whether your practice's sanction policies focus on workforce members who fail to comply with the security policies and procedures.

Consider whether your practice implements and enforces sanction policies to enforce the organization's policies to safeguard ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to hold workforce members accountable (and take appropriate disciplinary action) if it does not have documented policies, procedures, and processes for disciplining those who violated the security policies and procedures put into place to safeguard your practice's ePHI,

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

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
[45 CFR §164.308(a)(1)(ii)(C)]

Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures. The process should involve documenting when a formal employee sanctions process is initiated to include identifying the individual sanctioned and the associated reason.
[NIST SP 800-53 PS-8]

A10 - §164.308(a)(1)(ii)(C) Required Does your practice include its sanction policies and procedures as part of its security awareness and training program for all workforce members?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to notify your workforce about your policy and procedure to sanction workforce members who fail to comply with your practice's ePHI safeguards. Your sanctions policies could include a range of progressive disciplinary actions to fit the member's compliance failure, from re-training to termination of employment.

Possible Threats and Vulnerabilities:

Your practice may not be able to fully communicate the consequences of violating security policies to workforce members if its security and training program does not include sanction policies and procedures.

Such an omission could impact your practice in that the members of its workforce may not understand the severity of the consequences of violating security policies, hence making your practice vulnerable to violations.

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

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
[45 CFR §164.308(a)(1)(ii)(C)]

Document processes for organizational sanctions that reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. These processes should be described within access agreements, general personnel policies and procedures, and security awareness and training programs for all workforce members.
NIST SP 800-53 PS-8]

A11 - §164.308(a)(1)(ii)(D) Required Does your practice have policies and procedures for the review of information system activity?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that information system activity reviews enable your practice to detect and investigate irregular system use that can indicate a violation of security policies and a privacy breach.

Consider whether your practice:

- Analyzes its activity and incident reports
- Analyzes its audit reviews
- Reviews its exception reports
- Reviews its audit logs

Possible Threats and Vulnerabilities:

Your practice may not be able to detect and prevent security violations or unauthorized uses and disclosures of ePHI if it does not have policies and procedures for reviewing information system activity.

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:

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

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
[45 CFR §164.308(a)(1)(ii)(D)]

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

A12 - §164.308(a)(1)(ii)(D) Required Does your practice regularly review information system activity?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice reviews information system activity as part of its continuous, day-to-day operations.

Possible Threats and Vulnerabilities:

Your practice may not be able to detect and prevent security violations and privacy breaches related to ePHI if it does not review system activity information as part of its continuous, day-to-day operations.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
[45 CFR §164.308(a)(1)(ii)(D)]

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 while not altering the original content or time ordering of audit records.
[NIST SP 800-53 AU-7]

Monitor information systems to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections. Deploy monitoring devices to identify unauthorized use of information systems.
[NIST SP 800-53 SI-4]

A13 - §164.308(a)(2) Required Does your practice have a senior-level person whose job it is to develop and implement security policies and procedures or act as a security point of contact?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's primary contact for security is senior enough to influence its decision makers.

Consider that security includes responsibility for:

- Workforce security
- Vendor management
- Facility security
- Information system security

Possible Threats and Vulnerabilities:

You may not be able to influence your practice's decision makers to reduce risk to ePHI if it does not have a senior-level person who is responsible for developing and implementing security policies and procedures.

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. [45 CFR §164.308(a)(2)]

Assign a senior-level executive or manager as the authorizing official for information systems and ensure that individual authorizes the information system for processing before commencing operations.

[NIST SP 800-53 CA-6]

A14 - §164.308(a)(2) Required Is your practice's security point of contact qualified to assess its security protections as well as serve as the point of contact for security policies, procedures, monitoring, and training?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's primary contact for security has the knowledge and expertise to perform security responsibilities.

Consider that some certifications held by information security professional are Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).

Possible Threats and Vulnerabilities:

You may not be able to effectively implement safeguards to secure and protect ePHI if your practice's security point of contact is not qualified to complete a security risk analysis and also serve as the contact for security policies, procedures, monitoring, and training.

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, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.
- Unauthorized and inappropriate system activity and ePHI access can go undetected.

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
[45 CFR §164.308(a)(2)]

Assign a senior-level executive or manager as the authorizing official for information systems and ensure that individual authorizes the information system for processing before commencing operations.
[NIST SP 800-53 CA-6]

A15 - §164.308(a)(2) Required Does your practice have a job description for its security point of contact that includes that person's duties, authority, and accountability?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's primary contact for security has the knowledge and expertise to perform security responsibilities, such as:

- Being the primary contact for all security matters
- Periodically completing a risk analysis
- Advising on current system capabilities, vulnerabilities, and leading practices for mitigation
- Implementing policies and procedures for security
- Communicating and educating about security policies and procedures
- Helping management decide on security purchases (products and services)
- Assuring the security of information system security
- Verifying settings for hardware and software are activated
- Reviewing records of information system activity, such as audit logs, access reports, and security incident tracking reports on a regular basis.
- Participating in workforce security
- Supporting vendor management
- Supervising information system maintenance activities (whether completed by members of your workforce or vendors)
- Supporting facility security planning
- Supporting continuity planning
- Supporting plans for emergency mode of operations (including access to ePHI)
- Supporting information and information system recovery and resumption of routine practice operation after an emergency

Possible Threats and Vulnerabilities:

Your practice may not be able to effectively implement and manage security safeguards if it does not have a job description for its security point of contact that includes that person's duties, authority, and accountability.

Examples of Safeguards:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.
Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. [45 CFR §164.308(a)(2)]

Assign a senior-level executive or manager as the authorizing official for information systems and ensure that individual authorizes the information system for processing before commencing operations.
[NIST SP 800-53 CA-6]

A16 - §164.308(a)(2) Required Does your practice make sure that its workforce members and others with authorized access to your ePHI know the name and contact information for its security point of contact and know to contact this person if there are any security problems?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's awareness materials include the name and contact information for its security point of contact, such as posters, email reminders, and policy manuals.

Possible Threats and Vulnerabilities:

If your practice's workforce members do not know the name and contact information of the security point of contact, they may not be able to execute immediate and appropriate mitigating actions when there are security problems.

This could impact your practice's ability to respond to security incidents when they occur if your workface members do not know who to contact.

Examples of Safeguards:

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
[45 CFR §164.308(a)(2)]

Provide incident response training to workforce members consistent with assigned roles and responsibilities.
[NIST SP 800-53 IR-2]

Require workforce members to report suspected security incidents and/or problems to your practice's assigned security point of contact.
[NIST SP 800-53 IR-6]

A17 - §164.308(a)(3)(i) Required Does your practice have a list that includes all members of its workforce, the roles assigned to each, and the corresponding access that each role enables for your practice's facilities, information systems, electronic devices, and 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:

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

Related Information:

Things to Consider to Help Answer the Question:

The definition of workforce includes employees, volunteers, and trainees.

Consider whether your workforce members who are authorized to access ePHI have a unique identifier, and their role and corresponding access to ePHI is the minimum necessary to carry out their duties.

Possible Threats and Vulnerabilities:

Individuals without a need to know can access your practice's ePHI if it does not have a list that includes all members of its workforce, the roles assigned to each, and the corresponding access privileges for each role (including information systems, electronic devices, and 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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
[45 CFR §164.308(a)(3)(i)]

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

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 for individuals 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]

A18 - §164.308(a)(3)(i) Required Does your practice know all business associates and the access that each requires for your practice's facilities, information systems, electronic devices, and 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:

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

Related Information:

Things to Consider to Help Answer the Question:

A business associate is a person or an entity other than a workforce member of the covered entity who performs functions or activities or provides certain services to a covered entity that involve access by the business associate to ePHI.

Consider whether your practice has a list of all authorized maintenance companies and their employees who service your practice's facilities and its information systems.

Also consider whether your practice has a list of all information technology (IT) service providers and their employees (business associates) who provide information system services, such as cloud-based data backup and electronic health record (EHR) providers.

Possible Threats and Vulnerabilities:

Workforce members and business associates can have inappropriate or unauthorized access to your practice's ePHI if it does not have a list of all workforce members and business associates and the access privileges that are assigned to each for your practice's facilities, information systems, electronic devices, and ePHI.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
[45 CFR §164.308(a)(3)(i)]

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

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 for individuals 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]

A19 - §164.308(a)(3)(i) Required Does your practice clearly define roles and responsibilities along logical lines and assures that no one person has too much authority for determining who can access your practice's facilities, information systems, and 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice clearly defines roles and responsibilities along logical lines and assures that no single role is too inclusive. For example, a workforce member responsible for reviewing access logs is also the workforce member whose primary responsibilities are updating patient records. In this situation, the workforce member is essentially left to monitor his or her own use of information systems and access to ePHI, which may result in an impermissible/unauthorized access attempt by the same workforce member to go undetected.

Possible Threats and Vulnerabilities:

Workforce members and business associates can access your practice's ePHI if your it does not clearly define roles and responsibilities along logical lines and assures that no one person has too much authority for determining who can access your practice's facilities, information systems, and ePHI.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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.

<u>Examples of Safeguards:</u>
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
[45 CFR §164.308(a)(3)(i)]

Assign a senior-level executive or manager as the authorizing official for information systems and ensure that individual authorizes the information system for processing before commencing operations.
[NIST SP 800-53 CA-6]

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

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 for individuals 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]

A20 - §164.308(a)(3)(i) Required Does your practice have policies and procedures that make sure those who need access to ePHI have access and those who do not are denied such access?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice assigns access privileges based on the role performed by the use and the theories of least privileges and minimum necessary.

Possible Threats and Vulnerabilities:

Users might be assigned greater access privileges than is needed based on their individual roles and responsibilities if your practice does not have policies that explain how a user's need to know is verified before the least privileges are granted.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph

(a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
[45 CFR §164.308(a)(3)(i)]

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

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 for individuals 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]

A21 - §164.308(a)(3)(i) Required Has your practice chosen someone whose job duty is to decide who can access ePHI (and under what conditions) and to create ePHI access rules that others can follow?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice recognizes the importance of reviewing access requests and consider the trust it places in the person who is accountable for establishing access privileges.

Possible Threats and Vulnerabilities:

Your practice may not be able to identify the minimum necessary level of access for ePHI if it does not have an assigned workforce member whose job duty is to decide who can access ePHI (and under what conditions) and to create ePHI access rules that others can follow.

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, 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
[45 CFR §164.308(a)(3)(i)]

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

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 for individuals 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]

A22 - §164.308(a)(3)(ii)(A) Addressable Does your practice define roles and job duties for all job functions and keep written job descriptions that clearly set forth the qualifications?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has defined its roles and responsibilities to include the access authorizations (privileges) and other attributes for each workforce member and entity that will access its information systems and ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to effectively implement and manage security safeguards if it does not define roles and job duties for all of the organization's job functions and also keep written job descriptions that clearly set forth the qualifications.

Some potential impacts include:

- Workforce members may not be held accountable for your practice's overall security program.

- 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, loss, or theft of ePHI can lead to medical identity theft.
- Accurate ePHI may not be timely available, which can adversely impact your healthcare professionals' ability to diagnose and treat the patient.

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

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
[45 CFR §164.308(a)(3)(ii)(A)]

Develop, document and disseminate a formal access control policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should include procedures to facilitate its implementation and associated controls.
[NIST SP 800-53 AC-1]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should include procedures to facilitate its implementation and associated personnel security controls.
[NIST SP 800-53 PS-1]

A23 - §164.308(a)(3)(ii)(A) Addressable Does your practice have policies and procedures for access authorization that support segregation of duties?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice effectively deals with situations in which a workforce member might be able to approve his or her own access privileges by requiring a second person to approve the access authorization.

Possible Threats and Vulnerabilities:

You may not be able to effectively implement independent access authorization for all user requests if your practice does not have policies and procedures for access authorization that support segregation of duties.

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

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
[45 CFR §164.308(a)(3)(ii)(A)]

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

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]

Develop processes that implement security safeguards that restrict access to digital or non-digital media containing ePHI.
[NIST SP 800-53 MP-2]

A24 - §164.308(a)(3)(ii)(A) Addressable Does your practice implement procedures for authorizing users and changing authorization permissions?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice requires management supervision and approval before a user account can be created, modified, disabled, and removed.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard user account management against security violations if it does not implement procedures for authorizing and changing user privileges.

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.

<u>Examples of Safeguards:</u>
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
[45 CFR §164.308(a)(3)(ii)(A)]

Establish processes to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and periodically review and update the signed access agreements.
[NIST SP 800-53 PS-6]

Develop procedures to:

- Specify authorized users of the information system, group and role membership, and account privileges for each account.
- Create, enable, modify, disable, and remove accounts.
- Notify account managers when accounts are no longer required, access requirements change, workforce members are terminated, information system usage or need-to-know changes.
- Associate access authorizations and other attributes with each information system account.

[NIST SP 800-53 AC-2]

A25 - §164.308(a)(3)(ii)(A) Addressable Do your practice's policies and procedures for access authorization address the needs of those who are not members of its workforce?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's access authorization policies consider the needs of:

- Maintenance personnel
- Service providers
- Other business associates

Possible Threats and Vulnerabilities:

Your practice's policies and procedures for access authorization must address when and how to grant access privileges to business associates who need access to perform permitted business activities.

Examples of Safeguards:

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

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
[45 CFR §164.308(a)(3)(ii)(A)]

Develop processes to establish and maintain a list of authorized maintenance organizations or personnel which identifies their level of access to facilities, information systems, and ePHI.
[NIST SP 800-53 MA-5]

Develop processes to establish and monitor the security roles and responsibilities of 3rd party providers who access the practice facilities, information systems, and ePHI.
[NIST SP 800-53 PS-7]

A26 - §164.308(a)(3)(ii)(B) Addressable Does your organization have policies and procedures that authorize members of your workforce to have access to ePHI and describe the types of access that are permitted?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice only enables access to ePHI by determining the least access to ePHI that is necessary for the workforce member or service provider to perform the roles and responsibilities assigned.

Examples of least privileges and minimum necessary access questions are:

- What facilities need to be accessed and at what times?
- What information systems need to be accessed and at what times?
- Is remote access to information systems necessary and appropriate?
- Is access from an electronic device (laptop, tablet, smart phone and the like) necessary and appropriate?
- Under what circumstances must access be supervised?

Possible Threats and Vulnerabilities:

Individuals without a need to know could access your practice's ePHI if it does not have policies and procedures that authorize workforce members to have access to ePHI and describe the types of access that are permitted.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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:

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

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
[45 CFR §164.308(a)(3)(ii)(B)]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also include procedures to facilitate its implementation and associated personnel security controls.
[NIST SP 800-53 PS-1]

Establish processes to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and periodically review and update the signed access agreements.
[NIST SP 800-53 PS-6]

A27 - §164.308(a)(3)(ii)(B) Addressable Do your practice's policies and procedures require screening workforce members prior to enabling access to its facilities, information systems, and ePHI to verify that users are trustworthy?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice verifies the education level, degrees, professional certifications, and criminal history of workforce members.

Possible Threats and Vulnerabilities:

Unqualified or untrustworthy users could access your practice's ePHI if its policies and procedures do not require screening workforce members prior to enabling access to its facilities, information systems, and ePHI to verify that individuals are trustworthy.

Some potential impacts include:

- Unauthorized or excessive access to ePHI by individuals 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:

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

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
[45 CFR §164.308(a)(3)(ii)(B)]

Establish risk designations and screening criteria for each position category that a workforce member is assigned to based on the risk posed by their level of access to facilities, information systems, and ePHI.
[NIST SP 800-53 PS-2]

Develop policies and procedures for screening individuals prior to authorizing their access to the information system.
[NIST SP 800-53 PS-3]

A28 - §164.308(a)(3)(ii)(C) Addressable Does your practice have policies and procedures for terminating authorized access to its facilities, information systems, and ePHI once the need for access no longer exists?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's policies and procedures address circumstances in which:

- Its agreement with a business associate expires or is terminated for cause and the entity no longer needs access
- A workforce member's role changes
- Your practice determines, based on the findings of a risk assessment, that access privileges should be changed
- A workforce member's employment is terminated (whether by the practice or by the employee and whether such termination is hostile or amiable)

Possible Threats and Vulnerabilities:

Individuals without a need to know can access your practice's ePHI if it does not have policies and procedures for terminating authorized access to its facilities, information systems, and ePHI once the need for access no longer exists,

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
[45 CFR §164.308(a)(3)(ii)(C)]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also include procedures to facilitate its implementation and associated personnel security controls
[NIST SP 800-53 PS-1]

Develop policies and procedures to terminate access, retrieve all security-related organizational information, system-related property, and/or retain administrative access to information systems from workforce members when their need to access the facilities, information systems, and ePHI no longer exists.
[NIST SP 800-53 PS-4]

Periodically review current and on-going logical and physical access authorizations to information systems and facilities for workforce members, and modify access based on their new roles and operational needs when they are reassigned or transferred.
[NIST SP 800-53 PS-5]

A29 - §164.308(a)(3)(ii)(C) Addressable Does your practice have formal policies and policies and procedures to support when a workforce member's employment is terminated and/or a relationship with a business associate is terminated?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's policies and procedures require the:

- Disabling of access to facilities and information systems
- Revoking authentication credentials and mechanisms
- Conducting of exit interviews that remind the entity of continuing obligations, especially those for confidentiality
- Collecting all information systems, electronic devices and ePHI that might be in the entity's possession or control

Possible Threats and Vulnerabilities:

Former workforce members and service providers can access your practice's ePHI if it does not have policies and procedures for terminating authorized access to its facilities, information systems, and ePHI once the need for access no longer exists.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.
[45 CFR §164.308(a)(3)(ii)(C)]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also include procedures to facilitate its implementation and associated personnel security controls
[NIST SP 800-53 PS-1]

Develop policies and procedures to terminate access, retrieve all security-related organizational information, system-related property, and/or retain administrative access to information systems from workforce members when their need to access the facilities, information systems, and ePHI no longer exists.

A30 - §164.308(a)(4)(i) Standard Do your practice's policies and procedures describe the methods it uses to limit access to its 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that access protection methods include various methods of controlling access that can be based on:

- Identity
- Role

- Biometric
- Proximity
- A combination of access methods

Possible Threats and Vulnerabilities:

Your practice may not be able to protect ePHI against security violations if it does not implement a method of controlling access that is:

- Identity-based
- Role-based
- Biometric-based
- Proximity-based
- A combination of access methods.

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 for authorizing access to electronic protected health information that ate consistent with the applicable requirements of subpart E of this part.
[45 CFR §164.308(a)(4)(i)]

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

Develop procedures to:

- Specify authorized users of the information system, group and role membership, and account privileges for each account.
- Create, enable, modify, disable, and remove accounts.

- Notify account managers when accounts are no longer required, access requirements change, workforce members are terminated, information system usage and need-to-know changes.
- Associate access authorizations and other attributes with each information system account.

[NIST SP 800-53 AC-2]

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 for individuals 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]

A31 - §164.308(a)(4)(ii)(B) Does your practice have policies and procedures that explain how it grants access to ePHI to its workforce members and to other entities (business associates)?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that ePHI is accessed through workstations, software, programs, processes and mechanisms.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard ePHI against inappropriate or unauthorized use or disclosures if it does not have policies and procedures for authorizing and changing user access privileges to its workforce members and business associates.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
[45 CFR §164.308(a)(4)(ii)(B)]

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

Develop procedures to:

- Specify authorized users of the information system, group and role membership, and account privileges for each account.
- Create, enable, modify, disable, and remove accounts.
- Notify account managers when accounts are no longer required, access requirements change, workforce members are terminated, information system usage and need-to-know changes.
- Associate access authorizations and other attributes with each information system account. [NIST SP 800-53 AC-2]
- Employ the principles of least privilege/minimum necessary access for individuals 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]

A32 - §164.308(a)(4)(ii)(C) Addressable Do the roles and responsibilities assigned to your practice's workforce members support and enforce segregation of duties?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Segregation of duties means that duties for (a) determining, (b) assigning, and (c) enabling access to ePHI are performed by different people. In this way, no single person can establish an account, assign access credentials and turn on an individual's access to ePHI.

This built-in reliance on multiple people to enable access helps to reduce the risk of inappropriate access.

Possible Threats and Vulnerabilities:

If your practice does not segregate duties so that different workforce members are responsible for determining, assigning, and enabling access to ePHI then one person can make all of the decisions, which could cause inappropriate access to be granted

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that, based upon the covered entity's or business associate's access authorization policies, establish document, review, and modify a user's right of access to a workstation, transaction or program or process.
[45 CFR §164.308(a)(4)(ii)(C)]

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

Develop procedures to:

- Specify authorized users of the information system, group and role membership, and account privileges for each account.
- Create, enable, modify, disable, and remove accounts.
- Notify account managers when accounts are no longer required, access requirements change, workforce members are terminated, and information system usage or need-to-know changes.
- Associate access authorizations and other attributes with each information system account.

[NIST SP 800-53 AC-2]

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]

A33 - §164.308(a)(4)(ii)(C) Addressable Does your practice's policies and procedures explain how your practice assigns user authorizations (privileges), including the access that are permitted?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice only authorizes workforce members to have remote access, wireless access, access from electronic devices and the like when there is a need to do so based on the person's role and responsibilities.

Possible Threats and Vulnerabilities:

Workforce members without a need to have access from outside of the office and access from a mobile device, can access your practice's ePHI if it does not have policies and procedures for granting access based on their role and responsibilities.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that, based upon the entity's access authorization policies, establish document, review, and modify a user's right of access to a workstation, transaction or program or process.
[45 CFR §164.308(a)(4)(ii)(C)]

Develop, document, and disseminate to workforce members an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, the expected

coordination among organizational entities, and compliance requirements. This policy should include procedures to facilitate its implementation and the associated access controls.
[NIST SP 800-53 AC-1]

Develop procedures to:

- Specify authorized users of the information system, group and role membership, and account privileges for each account.
- Create, enable, modify, disable, and remove accounts.

A34 - §164.308(a)(5)(i) Standard Does your practice have a training program that makes each individual with access to ePHI aware of security measures to reduce the risk of improper access, uses, and disclosures?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that “awareness” requires communication and comprehension by the entire group of users who have access to the information system or ePHI. Some examples of security awareness activities could include:

- Motivational slogans
- Login access banners
- Videos
- Computer-based awareness materials
- Web-based awareness materials
- Posters or flyers
- Briefings, articles, newsletters, and magazines
- Exhibits

Training strives to produce relevant and needed (information) security skills and competencies relevant to the roles and responsibilities assigned to the workforce member and the information systems to which they are authorized to access.

Training content can include policies, procedures, tools, and other documents for the roles that your practice defined.

Consider whether your practice involves key stakeholders when preparing and maintaining its security awareness and training program, such as those responsible for human resources, privacy, and security.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not have a training program for its workforce members that outlines the various security measures for reducing the risk of improper access, uses, and disclosures

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:

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

Implement a security awareness and training program for all members of its workforce (including management).
[45 CFR §164.308(a)(5)(i)]

Develop, document, and disseminate to workforce members a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance, and procedures to facilitate the

implementation of the security awareness and training policy and associated security awareness and training controls. The policy should also include procedures to facilitate its implementation and associated personnel security controls
[NIST SP 800-53 AT-1]

A35 - §164.308(a)(5)(i) Standard Does your practice periodically review and update its security awareness and training program in response to changes in your organization, facilities or environment?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice understands that training is an ongoing, evolving process that responds to environmental and operational changes affecting the security of ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not periodically review and update its security awareness and training program in response to changes in organization, facilities or environment.

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

Implement a security awareness and training program for all members of its workforce (including management).
[45 CFR §164.308(a)(5)(i)]

Review and update the current security awareness and training policy and procedures based on environmental and operational changes affecting the security of ePHI.
[NIST SP 800-53 AT-1]

A36 - §164.308(a)(5)(i) Standard Does your practice provide ongoing basic security awareness to all workforce members, including physicians?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

A user is a person or entity with authorized access.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not educate its workforce members, including physicians, through ongoing basic security awareness trainings.

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

Implement a security awareness and training program for all members of its workforce (including management).
[45 CFR §164.308(a)(5)(i)]

Provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users (when required by information system changes, and thereafter on an ongoing basis).
[NIST SP 800-53 AT-2]

A37 - §164.308(a)(5)(i) Standard Does your practice provide role-based training to all new workforce members?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

A user is a person or entity with authorized access.

- Consider that what a workforce member needs to know about security in your practice can be both general and specific.
  - General knowledge is necessary for an understanding of foundation elements, such as terms and phrases, understanding privacy and security of ePHI is required by law, and everyone is expected to do their part. This is frequently referred to as "Awareness" activities.
  - Specific knowledge is necessary for the workforce member to understand how to perform the activities they are required to perform based on their role so that the privacy and security of ePHI can be established and maintained. This is frequently referred to as "Role-based Training" activities.
- Consider mandatory training for new hires to help make sure that all new hires have a general understanding of privacy and security and have the specific knowledge about how to perform the tasks assigned to them in a way that establishes and maintains privacy and security of ePHI.;
- Consider the value requiring "refresher" training on a periodic basis.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not provide mandatory role-based security training to new workforce members and periodic role-based security training for all other existing workforce members.

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:

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

Implement a security awareness and training program for all members of its workforce (including management).
[45 CFR §164.308(a)(5)(i)]

Provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties
(when required by information system changes, and thereafter on an ongoing basis).
[NIST SP 800-53 AT-3]

A38 - §164.308(a)(5)(i) Standard Does your practice keep records that detail when each workforce member satisfactorily completed periodic training?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice documents when the workforce member completes role-based HIPAA Security Rule training.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not maintain detailed records which include when workforce members periodically completed their role-based trainings.

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

Implement a security awareness and training program for all members of its workforce (including management).
[45 CFR §164.308(a)(5)(i)]

Document and monitor individual information system security training activities including basic security awareness training and specific information system security training. Retain individual training records for workforce members and business associates.
[NIST SP 800-53 AT-4]

A39 - §164.308(a)(5)(ii)(A) Addressable As part of your practice's ongoing security awareness activities, does your practice prepare and communicate periodic security reminders to communicate about new or important issues?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that people are the weakest link in your security program. They get busy, forget or try to cut corners to get things done faster. Periodic reminders can help to deter poor behaviors and reinforce good ones.

Consider that security reminders can be:

- Email reminders
- Meetings
- Posters
- Announcements that appear upon logging in

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not prepare and communicate periodic security reminders to communicate about new or important issues.

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

Periodic security updates.
[45 CFR §164.308(a)(5)(ii)(A)]

Disseminate security alerts, advisories, and directives to workforce members.
[NIST SP 800-53 SI-5]

A40 - §164.308(a)(5)(ii)(B) Addressable Does your practice's awareness and training content include information about the importance of implementing software patches and updating antivirus software when requested?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that:

- Software and firmware can have inherent weaknesses and flaws in their design. Manufacturers can identify these weaknesses and write code to improve them. These codes are commonly referred to as "patches."
- Timely implementation of software patches is a practice that can guard against malware by reducing the number of weaknesses that malware can exploit.
- Training workforce members to make updates to workstations and devices when requested to do so can help to reduce the risk presented by malware.
- Training workforce members not to load software to your practice's workstations and devices, without approval from the security official.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not educate its workforce about how to detect, report, and protect against malware.

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

Procedures for guarding against, detecting, and reporting malicious software.
[45 CFR §164.308(a)(5)(ii)(B)]

Establish procedures and oversight for installation of software by users; enforce software installation policies; and monitors policy compliance.
[NIST SP 800-53 CM-11]

A41 - §164.308(a)(5)(ii)(B) Addressable Does your practice's awareness and training content include information about how malware can get into your 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that malicious software can include viruses, worms, Trojans, time bombs, spyware, email hoaxes and the like.

Consider whether your practice's awareness and training content explains:

- The dangers presented by malware
- How to thwarting phishing schemes
- Why it is unsafe to click links contained in emails received from persons known and unknown
- Why opening attachments that are not scanned for malware is unsafe
- How to report such irregular system performance or suspicious communications.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if its workforce does not follow its policies and procedures for guarding against, detecting, and reporting malicious software and include malware protection.

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

Procedures for guarding against, detecting, and reporting malicious software.
[45 CFR §164.308(a)(5)(ii)(B)]

- Include practical exercises in security awareness and training that simulate:
  - Actual cyber-attacks
  - No-notice social engineering attempts to collect information
  - The adverse impact of opening malicious email attachments or invoking, via spear phishing attacks ,malicious web links

[NIST SP 800-53 AT-2]

A42 - §164.308(a)(5)(ii)(C) Addressable Does your practice include log-in monitoring as part of its awareness and training programs?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that monitoring information system log-in (and attempts to log-in) is one way to identify abuse of information systems and inappropriate access of ePHI.

Consider whether your practice makes its workforce members aware that:

- Their use of the practice's information systems (workstations and devices) and ePHI is being monitored

Misuse of information systems and ePHI will result in disciplinary action and may include termination of employment or more.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if its workforce members do not follow its policies and procedures regarding acceptable use of information systems and 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Procedures for monitoring log-in attempts and reporting discrepancies.
[45 CFR §164.308(a)(5)(ii)(C)]

Include information about monitoring log-in attempts and reporting discrepancies and include log-in monitoring as part of its awareness and training programs. Engage in practical exercises in security awareness training that simulate actual cyber-attacks (e.g., no-notice social engineering attempts to collect information), gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links
[NIST SP 800-53 AT-2]

Employ automated mechanisms and tools to assist in the tracking of security incidents and in the collection and analysis of incident information, such as malware attacks.
[NIST SP 800-53 IR-5]

A43 - §164.308(a)(5)(ii)(D) Addressable Does your practice include password management as part of its awareness and training programs?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's awareness and training educates its workforce about:

- How to select a password of suitable strength
- How to change a password
- The frequency with which a password should be changed
- The importance of not divulging or sharing passwords with others
- How to safeguard a password.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if its workforce is not aware does not have policies and procedures explaining how to create, change, and protect passwords and include password management as part of its awareness and training programs.

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:

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

Procedures for creating, changing, and safeguarding passwords.
[45 CFR §164.308(a)(5)(ii)(D)]

Develop, document, and disseminate to workforce members an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. This policy should

include procedures to facilitate its implementation and the associated access controls.
[NIST SP 800-53 AC-1]

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]

A44 - §164.308(a)(6)(i) Standard Does your practice have policies and procedures designed to help prevent, detect and respond to security incidents?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that an incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Consider whether your practice is able to timely and effectively recognize, report and respond to an incident.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not have policies and procedures designed to help prevent, detect and respond to security incidents.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 address security incidents.
[45 CFR §164.308(a)(6)(i)]

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

A45 - §164.308(a)(6)(ii) Required Does your practice have incident response policies and procedures that assign roles and responsibilities for incident response?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has implemented a process for responding to a security incident.

Consider that effective security incident procedures enable your practice to analyze, isolate, control, and recover from a security incident?

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not have incident response policies and procedures that assign roles and responsibilities for incident responses.

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
[45 CFR §164.308(a)(6)(ii)]

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

A46 - §164.308(a)(6)(ii) Required Does your practice identify members of its incident response team and assure workforce members are trained and that incident response plans are tested?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice:

- Identifies the roles that will participate in incident response and reporting
- Provides appropriate role-based training
- Engages in incident response testing
- Makes observations and recommendations for improving incident response in formal reports
- Identifies who may (and who may not) speak to business associates, patients, the media, and law enforcement in the event of an incident

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not identify members of its incident response team and assure workforce members are trained and that incident response plans are tested.

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
[45 CFR §164.308(a)(6)(ii)]

The organization provides incident response training to information system users consistent with assigned roles and responsibilities within a specific time period of assuming an incident response role or responsibility, (when required by information system changes, and thereafter on an ongoing basis).
[NIST SP 800-53 IR-2]

Test the incident response capability for the information systems to determine the incident response effectiveness and document the results.
[NIST SP 800-53 IR-3]

A47 - §164.308(a)(6)(ii) Required Does your practice's incident response plan align with its emergency operations and contingency plan, especially when it comes to prioritizing system recovery actions or events to restore key processes, systems, applications, electronic device and media, and information (such as 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice includes business continuity operating procedures, where applicable, to its incident response plan in order to standardize and prioritize system recovery actions or events.

Possible Threats and Vulnerabilities:

If your practice's incident response plan does not align with its emergency operations and contingency plan, it may not be able to safeguard its information systems, applications, and 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
[45 CFR §164.308(a)(6)(ii)]

Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing

incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
[NIST SP 800-53 IR-4]

A48 - §164.308(a)(6)(ii) Required Does your practice implement the information system's security protection tools to protect against malware?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice completes regular and real-time scans of its servers, information systems, and workstations, laptops and other electronic devices in order to identify and respond to suspected or known security incidents.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not implement the information system's security protection tools to protect against malware.

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
[45 CFR §164.308(a)(6)(ii)]

Employs automated mechanisms and tools to assist in the tracking of security incidents and in the collection and analysis of incident information, such as malware attacks.
[NIST SP 800-53 IR-5]

A49 - §164.308(a)(7)(i) Standard Does your practice know what critical services and ePHI it must have available to support decision making about a patient's treatment during an emergency?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that critical services can include creating, accessing, transmitting and storing ePHI, such as access and transmitting of ePHI for prescription medications.

Possible Threats and Vulnerabilities:

Your practice may not be able to operate and treat patients effectively and efficiently if it does not know what critical services and ePHI it must have available to support patient treatment decision making during an emergency.

Some potential impacts include:

- 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
[45 CFR §164.308(a)(7)(i)]

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]

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]

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]

A50 - §164.308(a)(7)(i) Standard Does your practice consider how natural or man-made disasters could damage its information systems or prevent access to ePHI and develop policies and procedures for responding to such a situation?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice's contingency plan includes provisions:

- Defining the organization's overall contingency objectives
- Establishing the organizational framework, roles, responsibilities, authority, and accountability
- Addressing scope, resource requirements, training, testing, plan maintenance, and backup requirements
- Activating an emergency mode of operations and enabling emergency access to ePHI
- Recovering from an emergency and resuming normal operations.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not know how natural or man-made disasters could damage its information systems or prevent access to ePHI; and develop policies and procedures for responding to such a situation.

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
[45 CFR §164.308(a)(7)(i)]

Consider whether your practice's continuity plan aligns with published expertise for business continuity such as NIST SP 800-34.

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]

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]

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]

A51 - §164.308(a)(7)(i) Standard Does your practice regularly review/update its contingency plan as appropriate?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice updates its contingency plan in response to changes in its environment, operations, or policies.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems, applications, and ePHI if it does not update its contingency plan in response to changes in its environment, operations, or policies.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
[45 CFR §164.308(a)(7)(i)]

Review and update the current contingency planning policy and contingency planning procedures regularly or as needed.
[NIST SP 800-53 CP-1]

A52 - §164.308(a)(7)(ii)(A) Required Does your practice have policies and procedures for the creation and secure storage of an electronic copy of ePHI that would be used in the case of system breakdown or 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that a data backup plan is a collection of procedures to create and maintain retrievable exact copies of ePHI.

Consider that retrievable exact copies of ePHI can be created and maintained in removable media (e.g. compact disks (CDs), universal serial bus (USB) Drives, Portable Disk Drives),or virtually (e.g. cloud-based storage).

Consider how you might protect your backup from unauthorized use or disclosures (e.g. encryption).

Possible Threats and Vulnerabilities:

Your practice may not be able to operate and treat patients effectively and efficiently if it does not have policies and procedures for the creation and secure storage of an electronic copy of ePHI that would be used in the case of system breakdown or disaster.

Some potential impacts include:

- 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:

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

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
[45 CFR §164.308(a)(7)(ii)(A)]

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]

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]

A53 - §164.308(a)(7)(ii)(B) Required Does your practice have policies and procedures for contingency plans to provide access to ePHI to continue operations after a natural or human-made 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice's ability to continue operating in the event of a disaster is dependent upon its ability to:

- Provide an alternative location for your practice's operation, such as location equipped with the information systems necessary to access ePHI to which key workforce members are instructed to report
- Provide information systems equipped to access ePHI
- Enable emergency access to ePHI
- Provide telecommunication services (including internet access)
- Enable recovery information systems and resumption of normal operations

Possible Threats and Vulnerabilities:

Your practice may not be able to continue operations and provide service to patients if it does not have policies and procedures for contingency plans to provide access to ePHI to continue operations after a disaster.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 to restore any loss of data.
[45 CFR §164.308(a)(7)(ii)(B)]

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]

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]

A54 - §164.308(a)(7)(ii)(C) Required Does your practice have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of ePHI immediately after a crisis situation?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that an emergency mode of operation plan enables your practice to secure and protect ePHI during the emergency.

Consider whether activities such as your practices access controls (identification and authentication of information system users), access logging, encryption, and data backup still function during its emergency operation.

Possible Threats and Vulnerabilities:

Your practice may not be able to continue operations and provide service to patients if it does not have an emergency mode of operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of ePHI immediately after a crisis situation.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
[45 CFR §164.308(a)(7)(ii)(C)]

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]

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

A55 - §164.308(a)(7)(ii)(D) Addressable Does your practice have policies and procedures for testing its contingency plans on a periodic basis?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice's contingency plan includes its data backup plan, disaster recovery plan, and emergency mode of operations plan.

Possible Threats and Vulnerabilities:

Your practice may not be able to continue operations and provide service to patients if it does not have policies and procedures for testing its contingency plans on a periodic basis.

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

Implement procedures for periodic testing and revisions of contingency plans.
[45 CFR §164.308(a)(7)(ii)(D)]

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]

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

A56 - §164.308(a)(7)(ii)(E) Addressable Does your practice implement procedures for identifying and assessing the criticality of its information system applications and the storage of data containing ePHI that would be accessed through the implementation of its contingency plans?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that understanding the criticality of information and information systems can enable your practice to adjust the scope of its contingency plans and prioritize its contingency activities.

Consider whether your practice has evaluated the criticality of its information systems by determining the type of information it stores.

Possible Threats and Vulnerabilities:

Your practice may not be able to continue operations and provide service to patients if it does not implement procedures for identifying and assessing the criticality of its information system applications and the storage of data containing ePHI that would be accessed through the implementation of its contingency plans

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

Assess the relative criticality of specific applications and data in support of other contingency plan components.
[45 CFR §164.308(a)(7)(ii)(E)]

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]

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]

Categorize information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.
[NIST SP 800-53 RA-2]

Document the security categorization results (including supporting rationale) in the security plan for the information system.
[NIST SP 800-53 RA-2]

Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.
[NIST SP 800-53 RA-2]

A57 - §164.308(a)(8) Standard Does your practice maintain and implement policies and procedures for assessing risk to ePHI and engaging in a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of your practice's 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:

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

Related Information:

Things to Consider to Help Answer the Question:

The operation of a healthcare organization and its business needs are dynamic – always changing. Through periodic analyses of risk to its health information, your practice can adjust its policies and procedures to meet its changing needs.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI against risks due to environmental and operational changes if it does not engage in periodic evaluations, both technical and non-technical.

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

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
[45 CFR §164.308(a)(8)]

Develop, document, and disseminate to workforce members a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls.
[NIST SP 800-53 RA-1]

A58 - §164.308(a)(8) Standard Does your practice periodically monitor its physical environment, business operations, and information system to gauge the effectiveness of security safeguards?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that monitoring the performance of your procedures and practices enables you to determine when an activity is not effective. A monitoring strategy addresses such issues as:

- Configuration management
- Impact analysis, to determine the security impact of changes your information systems and operations
- Ongoing security control assessments to assure your practice is implementing leading practices.

Possible Threats and Vulnerabilities:

Your practice may not implement effective security safeguards to protect its ePHI if it does not periodically monitor its physical environment, business operations, and information systems.

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:

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

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the

extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
[45 CFR §164.308(a)(8)]

Monitor information systems to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections. Deploy monitoring devices to identify unauthorized use of information systems.
[NIST SP 800-53 SI-4]

Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents, review physical access log periodically, and coordinate results of reviews and investigations with the organizational incident response capability.
[NIST SP 800-53 PE-6]

A59 - §164.308(a)(8) Standard Does your practice identify the role responsible and accountable for assessing risk and engaging in ongoing evaluation, monitoring, and reporting?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has clearly defined roles and responsibilities for completing its periodic risk analyses risk and engaging in ongoing evaluation, monitoring, and reporting on the effectiveness of its safeguards.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI against risk if it does not identify who is accountable for assessing risk and engaging in ongoing evaluation, monitoring, and reporting on the effectiveness of its safeguards.

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

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
[45 CFR §164.308(a)(8)]

Develop, document, and disseminate to workforce members a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls.
[NIST SP 800-53 RA-1]

A60 - §164.308(b)(1) Standard Does your practice identify the role responsible and accountable for making sure that business associate agreements are in place before your practice enables a service provider to begin to create, access, store or transmit ePHI on your behalf?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your organization may have contractors performing many functions that are essential to the operation of your practice.

For example, temporary employment agencies, IT or technology providers, or other service providers

Consider whether your practice assigns a workforce member the responsibility for making sure that the practice has written assurances from each of these service providers that assure protection of ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not identify the role responsible and accountable for making sure that business associate agreements are in place before your practice enables a service provider to begin to create, access, store or transmit PHI on behalf of the practice.

Some potential impacts include:

- Service providers are unaware of the types of sensitive information that they will possess or control when performing the services on your behalf and fail to take reasonable care to protect the privacy and security of ePHI.
- 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor
[45 CFR §164.308(b)(1)]

Sample Business Associate Agreement From OCR
[http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html]

The requirements set forth in this agreement are baseline minimums. Further, you and your service provider can always contract for greater assurances than are required by law.

A61 - §164.308(b)(1) Standard Does your practice maintain a list of all of its service providers, indicating which have access to your practice's facilities, information systems and 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Knowing who provides services to your practice and the nature of the services is an important component of your security plan. For example: Consider that a list of service providers can enable your practice to determine who its business associates are and can highlight potential points of failure that need to be addressed in the its contingency planning. Examples of service providers include:

- Health Information Exchanges or other Health Information Organizations
- Electronic health record (EHR)vendors
- E-prescribing gateway
- Patient billing services
- Legal, accounting or administrative services

Consider that your practice's list of service providers should be accurate and up-to-date to be of value.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its facilities, information systems, and ePHI if it does not maintain a list of its service providers and track the access level and roles of each.

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:

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

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor
[45 CFR §164.308(b)(1)]

Develop processes to establish and maintain a list of authorized maintenance organizations or personnel which identifies their level of access to facilities, information systems, and ePHI.
[NIST SP 800-53 MA-5]

Develop processes to establish and monitor the security roles and responsibilities of 3rd party providers who access the practice facilities, information systems, and ePHI.
[NIST SP 800-53 PS-7]

A62 - §164.308(b)(1) Standard Does your practice have policies and implement procedures to assure it obtains business associate agreements?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice develops and maintains business associate agreements each time it enters into a relationship with a service provider or any vendor who is not a workforce member who will process, transmit or store ePHI on its behalf.

Possible Threats and Vulnerabilities:

Your practice's service providers might not be aware of their responsibilities for safeguarding your practice's facilities, information systems, and PHI if you does not have policies and implement procedures requiring business associate agreements.

When assurances for the protection of PHI are not in place with all service providers, potential impacts include:

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

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

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor
[45 CFR §164.308(b)(1)]

A63 - §164.308(b)(2) Required If your practice is the business associate of another covered entity and your practice has subcontractors performing activities to help carry out the activities that you have agreed to carry out for the other covered entity that involve ePHI, does your practice require these subcontractors to provide satisfactory assurances for the protection of the 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:

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

Related Information:

Things to Consider to Help Answer the Question:

While this might only rarely occur in small practices, consider that in circumstances when your practice is acting as a business associate for a covered entity, it must provide written satisfactory assurances to the covered entity. To comply with the baseline requirements of a business associate, your practice must obtain written satisfactory assurances from its subcontractors that will collect, use, or disclose ePHI.

Possible Threats and Vulnerabilities:

Your practice's service providers might not be aware of their responsibilities for safeguarding your practice's facilities, information systems, and ePHI if you do not have policies and implement procedures requiring business associate agreements.

When assurances for the protection of ePHI are not in place with all service providers, 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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
[45 CFR §164.308(b)(1)]

A64 - §164.308(b)(3) Required Does your practice execute business associate agreements when it has a contractor creating, transmitting or storing 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has a written agreement with its service provider setting forth the service provider's satisfactory assurances for its handling of ePHI.

Satisfactory assurances include but are not limited to:

- Limiting use of ePHI as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures of ePHI inconsistent with those provided for in the agreement must be reported to the covered entity, as much any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its facilities, information systems, and ePHI if your agreement does not require the service provider to provide adequate security safeguards.

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:

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

Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).
[45 CFR §164.308(b)(3)]

O1 - §164.314(a)(1)(i) Standard Does your practice assure that its business associate agreements include satisfactory assurances for safeguarding 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Satisfactory assurances include but are not limited to:

- Limiting the business associate's use or disclosure of ePHI to as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures of ePHI inconsistent with those provided for in the agreement must be reported to the covered entity, as must any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Possible Threats and Vulnerabilities:

Your business associate might not be satisfactorily safeguarding your practice's ePHI if it does not provide written satisfactory assurances in its agreement with you.

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

The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.
[45 CFR §164.314(a)(1)(i)]

Satisfactory assurances include but are not limited to:

- Limiting the business associate's use or disclosure of ePHI to as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures of ePHI inconsistent with those provided for in the agreement must be reported to the covered entity, as must any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

O2 - §164.314(a)(2)(i) Required Do the terms and conditions of your practice's business associate agreements state that the business associate will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the practice and timely report security incidents to your practice?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice's business associate agreements can identify what the business associate must address in its security program.

Satisfactory assurances include but are not limited to:

- Limiting the business associate's use or disclosure of ePHI to as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures of ePHI inconsistent with those provided for in the agreement must be reported to the covered entity, as must any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its information systems and ePHI if your practice's business associate is not required to provide satisfactory assurances for the protection of ePHI, obtain the same assurances from its subcontractors, and report security incidents (experienced by the business associate or its subcontractors) to you in a timely manner.

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

The contract must provide that the business associate will (A) comply with the applicable requirements of this subpart;(i.e. HIPAA Security Rule) (B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and, (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by §164.410.
[45 CFR §164.314(a)(2)(i)]

Satisfactory assurances include but are not limited to:

- Limiting use of PHI to as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures inconsistent with those provided for in the agreement must be reported to the covered entity, as must any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

O3 - §164.314(a)(2)(iii) Required If your practice is the business associate of a covered entity do the terms and conditions of your practice's business associate agreements state that your subcontractor (business associate) will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the covered entity?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that there might be occasions when your practice is the business associate of another covered entity. The terms of your practice's agreement with the covered entity should include assurances for how it will protect ePHI and require your practice to obtain the same assurances from its subcontractors.

Consider that the business associate is required to notify the CE of a breach that occur through the handling of ePHI when it is in the possession of its subcontractor.

Your practice needs to know when an incident occurs with its subcontractor so that it can take steps necessary to notify the covered entity and take other measures required under the Breach Notification Rule. See the OCR website for more information. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard a covered entity's ePHI if the terms and conditions of your practice's agreement with its subcontractor, do not require implementation of appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI and timely notification in the event of an incident or breach.

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

The requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.
[45 CFR §164.314(a)(2)(iii)]

Satisfactory assurances include but are not limited to:

- Limiting use of ePHI to as described in the agreement or as required by law
- Employing appropriate safeguards to prevent use or disclosure of ePHI other than provided for in the agreement
- Uses or disclosures inconsistent with those provided for in the agreement must be reported to the covered entity, as must any security incident of which it becomes aware

To view these and other satisfactory assurances, see the sample Business Associate Agreement at the OCR website

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

PO1 -§164.316(a) Standard Do your practice's processes enable the development and maintenance of policies and procedures that implement risk analysis, informed risk-based decision making for security risk mitigation, and effective mitigation and monitoring that protects the privacy, confidentiality, integrity, and availability of 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice has processes established that enable it to implement risk analysis, informed risk-based decision making for security risk mitigation, and effective mitigation and monitoring that protects the privacy, confidentiality, integrity, and availability of ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its ePHI if it does not have processes that enable the development and maintenance of policies and procedures that implement risk analysis, informed risk-based decision making for security risk mitigation, and effective mitigation and monitoring.

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:

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

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, (i.e. HIPAA Security Rule) taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart (i.e. HIPAA Security Rule).
[45 CFR §164.316(a)]

Develop, document, and disseminate to workforce members a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls.
[NIST SP 800-53 RA-1]

Document, review, and disseminate risk assessment results to members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified as a result of a risk assessment.
[NIST SP 800-53 RA-3]

PO2 - §164.316(b)(1)(i) Standard Does your practice assure that its policies and procedures are maintained in a manner consistent with other business records?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that written policies and procedures can be saved as written manuals or in electronic form.

Possible Threats and Vulnerabilities:

Your practice's workforce may not be able safeguard your facilities, information system, and ePHI if your practice does not preserve policies and procedures by maintaining them in written manuals or in electronic form.

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:

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

Maintain the policies and procedures implemented to comply with this subpart (i.e. HIPAA Security Rule) in written (which may be electronic) form.
[45 CFR §164.316(b)(1)(i)]

PO3 - §164.316(b)(1)(ii) Standard Does your practice assure that its other security program documentation is maintained in written manuals or in electronic form?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

In addition to policies and procedures, consider that other security program documentation should be maintained in written manuals or in electronic form:

- Plans (data back-up plans, emergency plans, contingency plans, recovery plans, and mitigation plans)
- Risk analyses and findings
- Access and audit logs
- Performance measurements and audit reports
- Expert advice and published authorities
- Awareness content
- Role-based training materials
- Employment agreements
- Vendor agreements

Possible Threats and Vulnerabilities:

Your practice may not be able safeguard its facilities, information system, and ePHI if it does not assure that its other security program documentation is maintained in written manuals or in electronic form.

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

If an action, activity or assessment is required by this subpart (i.e. HIPAA Security Rule) to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
[45 CFR §164.316(b)(1)(ii)]

Retain information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Information handling and retention requirements should cover the full life cycle of information, in some cases extending beyond the disposal of information systems.
[[NIST SP 800-53 SI-12]

PO4 - §164.316(b)(2)(i) Required Does your practice assure that its policies, procedures, and other security program documentation are retained for at least six (6) years from the date when it was created or last in effect, whichever is longer?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that retaining policies, procedures, and other security program documentation:

- Can help to demonstrate the maturation of your security program over time.
- Can provide evidence of due diligence during an audit.
- Can provide context to better understand the rules under which your practice was operating at a particular point in time.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its facilities, information system, and ePHI if it does not assure that its policies, procedures, and other security program documentation is retained for at least six (6) years from the date when it was created or last in effect, whichever is longer?

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

Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
[45 CFR §164.316(b)(2)(i)]

Retain information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Information handling and retention requirements should cover the full life cycle of information, in some cases extending beyond the disposal of information systems.
[NIST SP 800-53 SI-12]

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

PO5 - §164.316(b)(2)(ii) Required Does your practice assure that its policies, procedures and other security program documentation are available to those who need it to perform the responsibilities associated with their role?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that documentation only has value when the information it contains is accessible to those who need it.

Consider whether your practice makes its policies, procedures, plans, and strategy accessible to applicable workforce members.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its facilities, information systems, and ePHI if it does not assure that its policies, procedures and other security program documentation are available to those who need it to perform the responsibilities associated with their role.

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:

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

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
[45 CFR §164.316(b)(2)(ii)]

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]

PO6 - §164.316(b)(2)(iii) Required Does your practice assure that it periodically reviews and updates (when needed) its policies, procedures, and other security program documentation?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Change is constant. Understand the nature of change and its impact on your practice's workforce, business associates, subcontractors, information systems, and ePHI.

Consider whether your practice evaluates its policies and procedures on an annual basis or upon occurrence of a significant event, such as changes in its environment or operations that can impact the security of ePHI.

Possible Threats and Vulnerabilities:

Your practice may not be able to safeguard its facilities, information systems, and ePHI if it does not periodically review and update (when needed) its policies, procedures, and other security program documentation.

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

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.
[45 CFR §164.316(b)(2)(iii)]

Develop, document, and disseminate to workforce members a security planning policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation of the security planning policy and associated controls.
[NIST SP 800-53 PL-1]

Review and update the current security policy and security planning procedures.
[NIST SP 800-53 PL-2]

The Office of the National Coordinator for
Health Information Technology

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: March 2014

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 and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

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
ONC	The Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
RBAC	Role-based Access Control
SRA	Security Risk Assessment
SRA Tool	Security Risk Assessment Tool
USB	Universal Serial Bus

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:

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

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 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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 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:

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

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.

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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)]

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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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)(ii) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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)(ii) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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:

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

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:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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]

The Office of the National Coordinator for
Health Information Technology

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

Security Risk Assessment Tool
Physical Safeguards Content

Version Date: March 2014

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 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 and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

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
ONC	The Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
RBAC	Role-based Access Control
SRA	Security Risk Assessment
SRA Tool	Security Risk Assessment Tool
USB	Universal Serial Bus

PH1 - §164.310(a)(1) Standard Do you have an inventory of the physical systems, devices, and media in your office space that are used to store or contain 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Identify the areas where your practice has information systems and equipment that create, transmit, or store ePHI. Include all buildings and rooms within it that have data centers, areas where equipment is stored, IT administrative offices, workstation locations, and other sites.

Information systems normally include hardware, software, information, data, applications, and communications.

Possible Threats and Vulnerabilities:

If your practice does not have an inventory, you may not be able to identify all of the workstations, portable devices, or medical devices that collect, use, or store ePHI.

Some potential impacts include:

- Natural threats, such as hurricanes, tornadoes, and earthquakes, which can cause damage or loss of ePHI.
- Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure and loss or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Have policies and procedures that are designed to control physical access to information systems that have ePHI, including facilities and rooms within them where your information systems are located. [45 CFR §164.310(a)(1)]

Identify all facility locations that your practice owns, rents, or occupies, where ePHI is collected, created, processed, or stored so that your practice can:

Establish physical access control procedures to:

- Limit entrance to and exit of the facility using one or more physical access methods.
- Control access to areas within the facility that are designated as publicly accessible.
- Secure keys, combinations, and other physical access devices.

[NIST SP 800-53 PE-3]

Establish physical access authorization procedures to:

- Develop and maintain a list of individuals with authorized access to the facility.
- Issue authorization credentials.

[NIST SP 800-53 PE-2]

Establish policy and procedures to control access to ePHI data by output devices such as printers, fax machines, and copiers in order to prevent unauthorized individuals from obtaining the output.
[NIST SP 800-53 PE-5]

PH2 - §164.310(a)(1) Standard Do you have policies and procedures for the physical protection of your facilities and equipment? This includes controlling the environment inside the facility.

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Information technology is sensitive to heat, humidity, dampness, static electricity, dust, and other conditions. Consider whether your practice has policies and procedures to:

- Make sure the physical environment for your information technology is optimal, enabling your systems to operate as designed or expected
- Protect your facilities and information systems from unauthorized access, alteration, or destruction.

Possible Threats and Vulnerabilities:

If your practice does not have a response plan in place to protect your facilities and equipment, then your practice cannot be sure that safeguards are in place to protect your practice's ePHI.

Some potential impacts include:

• Environmental threats, such as power failure and temperature extremes, which can cause damage to your information systems.

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

Have a plan that is designed to control physical access to information systems that have ePHI, including the facilities and rooms within them where your information systems are located. [45 CFR §164.310(a)(1)]

Establish policies and procedures for physical and environmental protection.
[NIST SP 800-53 PE-1]

PH3 - §164.310(a)(1) Standard Do you have policies and procedures for the physical protection of your facilities and equipment? This includes controlling the environment inside the facility.

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

The environment and the culture in which your practice conducts its business can evolve over time. As a result, the steps that your practice takes to protect its facilities and information systems must change to address new vulnerabilities in its physical security and environmental protections.

Possible Threats and Vulnerabilities:

You may be vulnerable to environmental threats if you do not regularly review and update your practice's policies and procedures as your physical security or environment changes.

Some potential impacts include:

- Environmental threats, such as power surges and outages of heating, air conditioning, and air filtration systems, which can enable humidity and dust to compromise the functional integrity and performance of your practice's information systems.

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

Have policies and procedures that are designed to control physical access to information systems that have ePHI, including the facilities and rooms within them where your information systems are located. [45 CFR §164.310(a)(1)]

Remain current on your practice's physical and environmental protection needs so that your supporting polices are responsive.
[NIST SP 800-53 PE-1]

PH4 - §164.310(a)(1) Standard Do you have physical protections in place to manage physical security risks, such as a) locks on doors and windows and b) cameras in nonpublic areas to monitor all entrances and exits?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider whether your practice has physical protections for the rooms where your information systems are located, the building in which they are located, and the property where the building is situated. Physical protections are items such as door and window locks, fences, gates, and camera surveillance systems.

Possible Threats and Vulnerabilities:

Your ePHI could be accessed by unauthorized users if you do not use physical security methods and devices to protect your information systems and the premises where they are located.

Some potential impacts include:

- Human threats, such as physical access by an unauthorized user, which can compromise ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Have policies and procedures that are designed to control physical access to information systems that have ePHI, to include facilities and rooms where your information systems are located. [45 CFR §164.310(a)(1)]

Limit access to workstation locations and other information systems that process or store ePHI by establishing physical access control procedures. Protective measures could include locks on doors, windows, and gates; exterior fences; barriers; and monitoring/detection camera systems.
[NIST SP 800-53 PE-3]

PH5 - §164.310(a)(2)(i) Addressable Do you plan and coordinate physical (facilities) and technical (information systems, mobile devices, or workstations) security-related activities (such as testing) before doing such activities to reduce the impact on your practice assets and individuals?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Efficiencies can be achieved when you coordinate physical and information technology protections. Failing to do so can result in damage (or loss) suffered to your facility or your information systems.

Possible Threats and Vulnerabilities:

Your practice may be unable to recover from a disaster if you do not test facilities and the security-related activities of their information systems before executing them.

Some potential impacts include:

• Natural and environmental threats, such as fire, water, loss of power, and temperature extremes, which can compromise the function and integrity of your practice's information systems.

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

Have procedures in place for emergency situations that manage and allow access to facilities where ePHI is stored in order to support lost data recovery tasks, per the disaster recovery and emergency mode operations plan.
[45 CFR §165.310(a)(2)(i)]

Establish and periodically test your emergency procedures to:

Establish an alternate processing site to continue operations by:

• Having appropriate agreements to permit the transfer and resumption of information services.

- Ensuring required equipment and supplies are onsite.
- Ensuring applicable security safeguards are in place.

[NIST SP 800-53 CP-7]

When necessary, establish an Alternate Work Site, to continue operations that include:

- Security controls.
- Continuous monitoring of control effectiveness.
- Incident reporting and response.

[NIST SP 800-53 PE-17]

PH6 - §164.310(a)(2)(i) Addressable Have you developed policies and procedures that plan for your workforce (and your information technology service provider or contracted information technology support) to gain access to your facility and its ePHI during 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:

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

Related Information:

Things to Consider to Help Answer the Question:

In emergency situations, access to your ePHI and information systems may be critical to treating your patients and operating your practice.

Planning ahead helps make sure those who need access to your ePHI and information systems (your workforce, your information technology service provider, or contracted information technology support) can still have access, even in an emergency.

Consider the steps you have taken to make sure your practice continues to operate in the event of an emergency.

Possible Threats and Vulnerabilities:

You may not be able to provide medical services in the event of a disaster if your practice does not have a plan designed to enable its workforce members (and your information technology service provider or contracted information technology support) to have access to ePHI during an emergency.

Some potential impacts include:

- Natural and environmental threats, such as fire, water, loss of power, and temperature extremes, which can compromise the function and integrity of your practice's information systems.
- Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Have procedures in place for emergency situations. Enable access to facilities where ePHI is stored. Support recovery of lost data. Have back up access to your practice's disaster recovery and emergency mode operations plan.
[45 CFR §165.310(a)(2)(i)]

Prepare and maintain a Contingency Plan that addresses disaster recovery and emergency mode of operations. Make sure your plan includes:

- Roles and responsibilities.
- Periodic review and updating.
- Timely communication and distribution to relevant workforce members.

[NIST SP 800-53 CP-2]

PH7 - §164.310(a)(2)(i) Addressable If a disaster happens, does your practice have another way to get into your facility or offsite storage location to get your 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps your practice has taken to provide alternative arrangements that will enable your workforce and authorized third parties (such as your information technology service provider or contracted IT technical support) to access ePHI and information systems even in times of emergency or disaster. An example is maintaining a copy of your ePHI at another location.

Possible Threats and Vulnerabilities:

You may be unable to access ePHI when it's needed if your practice's workforce members, business associates, and service providers do not know how to access your facilities or offsite storage locations during a disaster.

Some potential impacts include:

• Natural and environmental threats, such as fire, water, loss of power, and temperature extremes, which can compromise the function and integrity of your practice's information systems.
• Human threats, such as an unauthorized user who can exploit a state of emergency to vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Have emergency situation procedures in place to manage and allow access to facilities where ePHI is stored. The procedures should support lost data recovery tasks, per the disaster recovery and emergency mode operations plan.
[45 CFR §165.310(a)(2)(i)]

Establish an offsite backup storage facility for ePHI. Establish the supporting policy and procedures to manage access to the alternate site in case of a disaster.

Store a copy of ePHI at an alternative location:

• Establish an alternate location conducive to storage and recovery of information system backup information.
• Make sure the alternate location includes the same information security safeguards as the primary site (such as enabling authorized user access).
(NIST SP 800-53 CP-6)

PH8 - §164.310(a)(2)(ii) Addressable Do you have policies and procedures for the protection of keys, combinations, and similar physical access controls?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps you might have taken to make sure that your keys and business records for access controls, such as passwords to card key systems and electronic door codes, are protected and only designated people have access.

Possible Threats and Vulnerabilities:

Unauthorized users could gain access to your facilities and its rooms that contain your information systems and ePHI if your practice does not protect its keys, combinations, and similar access control methods.

Some potential impacts include:

- Human threats, such as an unauthorized user or a disgruntled workforce member who can compromise ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Establish policies and procedures to protect the facility and its equipment from unauthorized physical access, tampering, and theft.
[45 CFR §164.310(a)(2)(ii)]

Prepare an inventory of the keys, combinations, access cards, doors, locks, and the like and indicate the authorized users who possess them.

Establish physical access control procedures to change combinations and keys at regular intervals and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
[NIST SP 800-53 PE-3]

PH9 - §164.310(a)(2)(ii) Addressable Do you have policies and procedures governing when to re-key locks or change combinations when, for example, a key is lost, a combination is compromised, or a workforce member is transferred or terminated?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that the methods you rely on to protect your facilities are still effective after an employee, business associate, or service provider transfers, quits, or is fired. Steps may include re-keying locks or changing combinations.

Possible Threats and Vulnerabilities:

Your practice is at risk of unauthorized users gaining access to your facilities and information system if you do not take steps to re-key locks or change combinations when an employee, business associate, or service provider with access transfers, resigns, or is terminated.

Some potential impacts include:

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

Examples of Safeguards:

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

Limit access to your practice's office and other locations where ePHI is located to only those workforce members and third parties who require access to do their jobs. [45 CFR §164.310(a)(1)]

Create and maintain facility access control policies and procedures. Limit physical access to only workforce members, business associates, patients, and other known visitors. Establish physical access control procedures to change combinations and keys at regular intervals and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. [NIST SP 800-53 PE-3]

PH10 - §164.310(a)(2)(ii) Addressable Do you have a written facility security plan?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

A facility security plan is a document containing policies and procedures designed to control access to the facility, maintain the facility, and control access to systems and equipment that handle ePHI.

Consider the steps that your practice has taken to document how your facilities can withstand foreseeable threat events, such as locks on doors and windows, earthquake and hurricane preparedness, surge protectors, and backup heating, cooling, and air filtration systems.

Possible Threats and Vulnerabilities:

Your practice cannot be sure of the policies, procedures, and safeguards to protect your practice's facility, information systems, and ePHI if your practice does not have a documented facility security plan to protect your facilities and equipment.

Some potential impacts include:

- Natural threats, such as hurricanes, tornadoes, floods, ice, and earthquakes, which can cause damage or loss of ePHI.
- Environmental threats, such as power surges and outages of heating, air conditioning, and air filtration systems, which can enable humidity and dust to compromise the functional integrity

and performance of your practice's information systems.

• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Establish policies and procedures to protect the facility and its equipment from unauthorized physical access, tampering, and theft.
[45 CFR §164.310(a)(2)(ii)]

As part of contingency planning, develop and document a facility security plan that includes:

• Policies and procedures for physical and environmental protection.
(NIST SP 800-53 PE-1)
• A system-level security plan. (NIST SP 800-53 PL-2)

PH11 - §164.310(a)(2)(ii) Addressable Do you take the steps necessary to implement your facility security plan?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice might have taken to put its policies and procedures into practice.

Possible Threats and Vulnerabilities:

Your practice cannot make sure that safeguards are in place to protect its information systems and ePHI if your practice does not take the steps necessary to carry out its facility security plan.

- Natural threats, such as hurricanes, tornadoes, floods, ice, and earthquakes, can cause damage or loss of ePHI.
- Environmental threats, such as power surges and outages of heating, air conditioning, and air filtration systems, can enable humidity and dust to compromise the functional integrity and performance of your practice's information systems.
- Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Establish policies and procedures to protect the facility and its equipment from unauthorized physical access, tampering, and theft.
[45 CFR §164.310(a)(2)(ii)]

As part of contingency planning, implement a facility security plan that includes:

- Policies and procedures for physical and environmental protection.

[NIST SP 800-53 PE-1]
• A system-level security plan.
[NIST SP 800-53 PL-2]

PH12 - §164.310(a)(2)(iii) Addressable Do you have a Facility User Access List of workforce members, business associates, and others who are authorized to access your facilities where ePHI and related information systems are located?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice needs to know who needs to access its facilities, when the access is necessary, the reason for the access, and how it can provide access before it can take the steps necessary to enable that access and deny access to others.

A Facility User Access List inventories the people who need access to your facilities.

Before making decisions about authorizing access to a facility, your practice needs to understand the role and function of the individual.

Consider that individuals can be workforce members, maintenance contractors, IT contractors (such as those accessing software programs for testing), probationary employees, interns, volunteers, and visitors.

<u>Possible Threats and Vulnerabilities:</u>

Your practice risks having unauthorized people access locations where your technology is located or having more access than is needed if you do not have a Facility User Access List that outlines the individuals with authorized admittance to a controlled area.

• Decisions about authorizing access should be based on the role or function of the individual in order to protect the integrity and confidentiality of ePHI.
• Human threats, such as an unauthorized user, can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

<u>Examples of Safeguards:</u>
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Implement procedures to control and validate a person's access to facilities based on role or function, including visitor control and access control to information systems.
[45 CFR §164.310(a)(2)(iii)]

Have policies and procedures in place to:

• Ensure information system access control policies are enforced.
[NIST SP 800-53 AC-3]

Establish physical access control procedures to:

• Enforce physical access authorizations at designated entry/exit points to the facility where the information system that contains the ePHI is located.
[NIST SP 800-53 PE-3]

PH13 - §164.310(a)(2)(iii) Addressable Do you periodically review and approve a Facility User Access List and authorization privileges, removing from the Access List personnel no longer requiring access?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

The effectiveness of your practice’s facility access controls is greatly dependent upon the accuracy of its Access List.

An Access List is a roster of individuals authorized admittance to a controlled area.

Consider your workforce members, maintenance contractors, and visitors (e.g., patients and sales representatives). Access to an area where there is ePHI or related information systems should be limited to those with a need for access to such areas.

Access controls must enable access to authorized workforce members and third parties with a validated need and deny access to all others.

Possible Threats and Vulnerabilities:

Your ePHI could be exposed to unauthorized users if your practice does not periodically update its Access List and authorization privileges.

Decisions about authorizing access should be based on the role or function of the user to protect the confidentiality, integrity, and availability of ePHI.

Some potential impacts include:

• Human threats, such as an unauthorized user who can compromise ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Implement procedures to control and validate a person's access to facilities based on role or function, including visitor control and control of access to information systems.
[45 CFR §164.310(a)(2)(iii)]

Establish physical access authorization procedures and conduct a periodic review and update of the Access List to remove users who no longer need access.
[NIST SP 800-53 PE-2]

PH14 - §164.310(a)(2)(iii) Addressable Does your practice have procedures to control and validate someone's access to your facilities based on that person's role or job duties?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that it only grants an individual access to its facilities based on a validated need and denies access to all others.

Possible Threats and Vulnerabilities:

Unauthorized users could gain access to your practice's information systems and ePHI if your practice does not have procedures to manage access to a facility based on user role and function.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement procedures to control and validate a person's access to facilities based on role or function, including visitor control and access control to information systems.
[45 CFR §164.310(a)(2)(iii)]

Develop policies and procedures to manage access to a facility based on roles and functions, including policies and procedures for physical and environmental protection. Include a formal and documented policy that addresses purpose, scope, roles, and responsibilities of an

individual.
[NIST SP 800-53 PE-1]

PH15 - §164.310(a)(2)(iii) Addressable Do you have procedures to create, maintain, and keep a log of who accesses your facilities (including visitors), when the access occurred, and the reason for the access?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider that your practice cannot make sure that its facility access controls are working unless it has a written record of those who enter/leave the facility. An access log is a written document detailing who enters and leaves the facility and their purpose.

Possible Threats and Vulnerabilities:

Unauthorized users may access your practice's information systems and ePHI. If your practice maintains a record of a) who enters the space where information systems and ePHI are maintained and b) the purpose for their entry, it will be better able to trace and account for possible or actual unauthorized access.

Some potential impacts include:

• Human threats, such as disgruntled workforce members or unauthorized users who can vandalize your practice's information systems. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement procedures to control and validate a person's access to facilities based on role or function, including visitor control and control of access to information systems.
[45 CFR §164.310(a)(2)(iii)]

Have a process for developing, maintaining, and periodically reviewing a record of individuals who visit your practice.
[NIST SP 800-53 PE-8]

PH16 - §164.310(a)(2)(iii) Addressable Has your practice determined whether monitoring equipment is needed to enforce your facility access control policies and procedures?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the valuable role that monitoring equipment (e.g., a key card reader, video camera, or motion sensor) can provide to help your practice make sure that facility access is controlled according to your practice's policies and procedures.

Possible Threats and Vulnerabilities:

If your practice does not monitor who enters and exits its facilities during or after business hours (by use of monitoring equipment such as cameras or alarm systems), then your practice cannot enforce access control policies and procedures; cannot know who is entering the facility(ies); and cannot trace and account for unauthorized users' access to your practice's ePHI and information systems.

Some potential impacts include:

• Human threats, such as disgruntled workforce members or unauthorized users who can vandalize your practice's information systems. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Implement procedures to control and validate a person's access to facilities based on role or function, including visitor control and control of access to information systems.
[45 CFR §164.310(a)(2)(iii)]

Establish procedures and implement monitoring tools to continuously monitor physical access to your facility where ePHI is stored. Periodically review the logs to verify no unauthorized access has occurred.
[NIST SP 800-53 PE-6]

PH17 - §164.310(a)(2)(iv) Addressable Do you have maintenance records that include the history of physical changes, upgrades, and other modifications for your facilities and the rooms where information systems and ePHI are kept?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider how your practice's business can evolve over time. For example, it can change locations or open another office. Knowing when your organization adds or closes facilities is important to an accurate and effective facility security plan in addition to records about maintenance and changes. For example, repurposing a file room for computer network servers or other technology might require you to address temperature and humidity controls, backup electrical service, surge protectors, air filtration, fire suppression systems, and door locks.

Possible Threats and Vulnerabilities:

You might be unaware of all the locations where ePHI is collected, processed, or stored, as well as the effectiveness of your security plan, if your practice does not keep a formal written record, which tracks maintenance and physical changes, upgrades, and other modifications to your facilities.

Some potential impacts include:

• Natural threats, such as hurricanes, tornadoes, floods, ice, and earthquakes, which can cause damage or loss of ePHI.
• Environmental threats, such as power surges and outages of heating, air conditioning, and air filtration systems, which can enable humidity and dust to compromise the functional integrity and performance of your practice’s information systems.
• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Have policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
[45 CFR §164.310(a)(2)(iv)]

Implement policies and procedures to document facility and information system maintenance (repairs and modifications) and review them on a regular basis.
[NIST SP 800-53 MA-2]

PH18 - §164.310(a)(2)(iv) Addressable Do you have a process to document the repairs and modifications made to the physical security features that protect the facility, administrative offices, and treatment areas?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

It is a sound business practice to keep records concerning installation and repairs to the physical components of a facility which are related to security (for example, computer hardware, walls, doors, and locks).

Possible Threats and Vulnerabilities:

You may be unaware of the status or effectiveness of the repairs and modifications intended to protect areas where ePHI is collected, processed, or stored if you do not have a process to document the repairs and modifications made to the physical security features that protect the facility, such as locks, doors, and keypads.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Have policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
[45 CFR §164.310(a)(2)(iv)]

Develop a process to maintain and track all of your practice's maintenance records or any modifications made to the physical security of the areas where ePHI is stored, such as system maintenance policies and procedures.
[NIST SP 800-53 MA-1]

Establish a timely maintenance process for your practice's information systems and facilities.
[NIST SP 800-53 MA-6]

PH19 - §164.310(b) Standard Does your practice keep an inventory and a location record of all of its workstation 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Workstation devices may refer to workstations, laptops, printers, copiers, tablets, smart phones, monitors, and others. Include information such as the type of workstation device, the capability of the workstation device, and the tasks that you commonly do on it.

Possible Threats and Vulnerabilities:

Your practice may not be aware of the environment in which the device is used if your practice does not keep an inventory and is not aware of the location of all of its workstations, laptops, printers, copiers, tablets, smart phones, monitors, and other electronic devices. ePHI can be exposed in a surrounding or environment that is not suitable for handling or accessing that information.

Some potential impacts include:

- Environmental threats, such as power surges and outages of heating, air conditioning, and air filtration systems, which can enable humidity and dust to compromise the functional integrity and performance of your practice's information systems.
- Human threats, such as unauthorized or malicious users who can take advantage of exposed ePHI and can therefore be used to commit identity fraud.

Examples of Safeguards:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

As part of your practice’s physical access control policies and procedures, create, maintain, and periodically review an inventory of all workstations and other electronic devices that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices). [NIST SP 800-53 PE-3]

PH20 - §164.310(b) Standard Has your practice developed and implemented workstation use policies and procedures?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the policies that your practice has in place that define the appropriate use and performance specifications for its workstations that have access to or process ePHI. Be sure to include all types of workstations, such as medical devices or diagnostic screening tools.

Possible Threats and Vulnerabilities:

Workforce members, business associates, services providers, and the general public may not be aware of how to use devices appropriately if your practice does not implement policy and procedures that define the expectations.

Some potential impacts include:

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

Examples of Safeguards:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

Develop policies and procedures to enforce access control policies that define the acceptable use of information systems, workstations, and other electronic devices that contain ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[NIST SP 800-53 AC-3]

PH21 - §164.310(b) Standard Has your practice documented how staff, employees, workforce members, and non-employees access your workstations?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

This refers to the secure access to workstation computer hardware, printers, network, disks, tapes, and other media. It also includes the ability or the means necessary to read, write, modify, or communicate ePHI. Non-employees include, for example, patients, volunteers, interns, visitors, contractors, service personnel, and the general public.

Possible Threats and Vulnerabilities:

Your practice cannot be sure its workstations and information system will be used appropriately if it does not define appropriate measures to restrict access to its workstations and information systems by its workforce members, business associates, services providers, and the general public.

Some potential impacts include:

• Human threats, such as unauthorized, malicious or untrained users who can vandalize or unintentionally compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

Develop guidelines on how to use the workstations and information systems that handle ePHI, such as:

• Establishing policy and procedures to control access of ePHI data by output devices.
[NIST SP 800-53 PE-5]

• Defining access agreements to manage access to information systems containing ePHI and requiring users to sign appropriate access agreements prior to being granted access.
[NIST SP 800-53 PS-6]

PH22 - §164.310(c) Standard Does your practice have policies and procedures that describe how to prevent unauthorized access of unattended workstations?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that non-employees, visitors, and patients are prevented from viewing another person's ePHI or operating workstations when its workforce members leave the workstation unattended.

Workstations may refer to desktop computers, laptops, printers, copiers, tablets, smart phones, monitors, and others. Include information such as the type of workstation device, the capability of the workstation device, and the tasks that you commonly use on it.

Possible Threats and Vulnerabilities:

Workstations with access to ePHI can be at risk of unauthorized access if your practice does not have and implement policies and procedures that describe how to prevent unauthorized access to unattended workstations and other electronic devices.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Establish policies and procedures for preventing unauthorized access to unattended workstations or electronic devices (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices) and information systems that handle ePHI. Include policies and procedures for:

- Establishing access control procedures for transmission medium.
[NIST SP 800-53 PE-4]

- Determining media access.
[NIST SP 800-53 MP-2]
- Marking media.
[NIST SP 800-53 MP-3]

PH23 - §164.310(c) Standard Does your practice have policies and procedures that describe how to position workstations to limit the ability of unauthorized individuals to view 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that the work environment is configured in a manner that inhibits non-employees, visitors, and patients from incidentally viewing another person's ePHI on workstations.

Workstations may refer to desktop computers, laptops, printers, copiers, tablets, smart phones, monitors, and others. Include information such as the type of workstation device, the capability of the workstation device, and the tasks that you commonly do on it.

Possible Threats and Vulnerabilities:

Workstations might incidentally/accidentally expose ePHI to unauthorized users if your practice's policies and procedures do not describe suitable workstation location and configuration. Workstation screens containing ePHI may be viewable at a distance or different angles to users who are not authorized for viewing.

Some potential impacts include:

- Human threats, such as an unauthorized or malicious user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Develop policies and procedures for the physical location of information system components (including the location, configuration, and positioning of workstations and other electronic devices) to prevent unauthorized access.
[NIST SP 800-53 PE-18]

PH24 - §164.310(c) Standard Have you put any of your practice's workstations in public areas?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Workstations may refer to desktop computers, laptops, printers, copiers, tablets, smart phones, monitors, and others. Include information such as the type of workstation device, the capability of the workstation device, and the tasks that you commonly do on it.

Possible Threats and Vulnerabilities:

There might be unauthorized access to ePHI if your practice places workstations in publicly accessible areas.

Some potential impacts include:

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

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Establish policies and procedures for storage media where ePHI is stored. For example, consider having a current list of locations within your practice that are not open to the public, and restrict storage media (workstations and other electronic devices) to such locations.
[NIST SP 800-53 MP-4]

PH25 - §164.310(c) Standard Does your practice use laptops and tablets as workstations? If so, does your practice have specific policies and procedures to safeguard these workstations?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Laptop, tablets, and smart phones can be used as workstations accessing ePHI.

Consider the policies and procedures that your practice put in place to make sure these devices are used in a manner that makes sure ePHI is not visible or accessible by unauthorized users.

Possible Threats and Vulnerabilities:

Mobile workstations may be more susceptible to incidental or unauthorized access than non-mobile workstations. Mobile workstation screens containing ePHI may be viewable at a distance or at different angles to unauthorized users.

Some potential impacts include:

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

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Develop policies and procedures to manage how (and where) ePHI is accessed via mobile devices (such as laptops, tablets, and mobile phones) and develop acceptable use and storage guidelines for your practice.
[NIST SP 800-53 MP-7]

PH26 - §164.310(c) Standard Does your practice have physical protections in place to secure your workstations?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Physical security safeguards include doors, locks, barriers, and keyed access systems.

Possible Threats and Vulnerabilities:

There may be unauthorized access to ePHI if your practice does not put physical security safeguards in place for all workstations. All workstations should be protected by physical security, such as doors, locks, barriers, and keyed access systems, to ensure that ePHI is accessed only by authorized users.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. [45 CFR §164.310(c)]

Implement processes to restrict unauthorized physical access to workstations and other electronic devices that handle ePHI, including output devices, such as printers and fax machines.
[NIST SP 800-53 PE-5]

PH27 - §164.310(c) Standard Do you regularly review your workstations' locations to see which areas are more vulnerable to unauthorized use, theft, or viewing of the data?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Many printers, copiers, and fax machines have built-in memory that stores the documents that workforce members print, copy, and fax. Further, many mobile devices, such as tablets, laptops, and smart phones, save viewed information in temporary files. Consider the steps you take to make sure that office equipment cannot be accessed by unauthorized users.

Possible Threats and Vulnerabilities:

Lack of regular monitoring and tracking of the movement of mobile and non-mobile devicesand office equipment may lead to undetected incidents involving unauthorized access to ePHI.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the confidentiality, integrity or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Conduct periodic review of the location of your information systems (such as workstations and components) to evaluate their vulnerability to access by unauthorized individuals.
[NIST SP 800-53 PE-18]

PH28 - §164.310(c) Standard Does your practice have physical protections and other security measures to reduce the chance for inappropriate access of ePHI through workstations? This could include using locked doors, screen barriers, cameras, and guards.

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Workstations may refer to desktop computers, laptops, printers, copiers, tablets, smart phones, monitors, and others. Include information such as the type of workstation device, the capability of the workstation device, and the tasks that you commonly do on it.

Possible Threats and Vulnerabilities:

There may be unauthorized access to ePHI if your practice does not strategically position all workstations behind physical security safeguards, such as locked doors and/or screen barriers. Workstation screens containing ePHI may be viewable at a distance or from different angles to users who are not authorized for viewing.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

As part of your security plan, establish physical access control policies and procedures designed to safeguard workstations and other electronic devices.
[NIST SP 800-53 PE-3]

PH29 - §164.310(c) Standard Do your policies and procedures set standards for workstations that are allowed to be used outside of your facility?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice has taken to make sure workstations that are routinely used outside of its facilities are used in a manner that reduces the risk of incidental viewing or unauthorized access of information systems and ePHI.

Possible Threats and Vulnerabilities:

Use of smart phones, tablets, and laptops from inappropriate locations may result in incidental disclosure or unauthorized access to ePHI if your practice does not set policies, procedures, and standards for acceptable workstation use outside of its facilities. Workstation screens containing ePHI may be viewable at a distance or from different angles to users who are not authorized for viewing, especially in public areas.

Some potential impacts include:

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

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

Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
[45 CFR §164.310(c)]

Develop policies and procedures for acceptable use and storage of electronic devices that are remotely accessing ePHI.
[NIST SP 800-53 MP-4]

PH30 - §164.310(d)(1) Standard Does your practice have security policies and procedures to physically protect and securely store electronic devices and media inside your facility(ies) until they can be securely disposed of or destroyed?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Storage media and devices take on many different forms, from portable hard drives to thumb drives that fit easily onto a key ring. While small, these devices can hold enormous amounts of electronic data. Consider the policies and procedures put in place by your practice to securely store and track movement of devices and electronic media in your facilities from the time they are acquired to the time they are destroyed.

Possible Threats and Vulnerabilities:

ePHI can be removed from your facilities without being observed and/or monitored if your practice does not have security policies and procedures to physically protect and securely store electronic devices and media.

Some potential impacts include:

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

Examples of Safeguards:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop a security policy for the protection and storage of your digital media, including a documented component inventory of information systems that contain ePHI [NIST SP 800-53 CM-8] and policies and procedures for:

• Storing media where ePHI is stored.
[NIST SP 800-53 MP-4]
• Protecting media that contain ePHI.
[NIST SP 800-53 MP-1]

• Accessing media that contain ePHI.
[NIST SP 800-53 MP-2]
• Marking the media where ePHI is stored.
[NIST SP 800-53 MP-3]

PH31 - §164.310(d)(1) Standard Do you remove or destroy ePHI from information technology devices and media prior to disposal of the device?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that the ePHI stored on electronic devices and media is deleted prior to disposal of the device.

Possible Threats and Vulnerabilities:

ePHI left in discarded devices and media can be accessed by malicious unauthorized users if you do not sanitize (remove) that information prior to disposal or destruction of the equipment.

Some potential impacts include:

• Human threats, such as an unauthorized user who can compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop a process for sanitizing and securely disposing of electronic devices and media that contain ePHI.
[NIST SP 800-53 MP-6]

PH32 - §164.310(d)(1) Standard Do you maintain records of the movement of electronic devices and media inside your facility?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Electronic devices and storage media can store vast amounts of ePHI. Consider the steps that your practice takes to make sure it knows where electronic devices and storage media are on a day-to-day basis, especially when they are moved internally within your practice area.

Possible Threats and Vulnerabilities:

You cannot effectively apply the policies designed to protect the confidentiality, integrity, and availability of ePHI if you do not maintain an inventory of what ePHI you maintain and where it resides (e.g., on electronic devices and media).

Some potential impacts include:

• Natural threats, such as hurricanes, tornadoes, snow, ice, floods, and earthquakes, which can cause damage to your facilities, resulting in loss of ePHI.
• Environmental threats, such as power failure and temperature extremes, which can cause damage to your information systems.
• Human threats, such as an unauthorized user who can vandalize or compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop and maintain an inventory of your storage media and/or information systems that handle ePHI. As part of your security plan for handling storage media, include policies and procedures for transportation of media where ePHI is stored.
[NIST SP 800-53 MP-5]

PH33 - §164.310(d)(1) Standard Have you developed and implemented policies and procedures that specify how your practice should dispose of electronic devices and media containing 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Electronic devices and media can contain significant amounts of ePHI, and secure disposal is very important. Consider the steps that your practice has taken to make sure that its electronic devices and media are disposed of in a manner that makes sure the confidentiality of ePHI is not compromised.

Possible Threats and Vulnerabilities:

ePHI can leave your facility and be accessed by an unauthorized user without your knowledge if you do not have policies and procedures in place that define how to properly sanitize and dispose of electronic devices and media. A malicious user can then use undeleted utilities to recover data from discarded media.

Some potential impacts include:

- Human threats, such as an unauthorized user who can compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

As part of your plan for disposing of electronic devices and media containing ePHI, include policies and procedures for the sanitization of media where ePHI is stored.
[NIST SP 800-53 MP-6]

PH34 - §164.310(d)(2)(i) Required Do you require that all ePHI is removed from equipment and media before you remove the equipment or media from your facilities for offsite maintenance or disposal?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

ePHI can be stored in photo copiers, smart phones, tablets, laptops, and a wide array of electronic devices and media. In some instances, it may not be readily apparent to the user that ePHI is there. Consider the steps that your practice has taken to make sure that its ePHI is identified and removed from equipment, workstations, and information systems before they are removed from the facility for maintenance or disposal.

Possible Threats and Vulnerabilities:

An unauthorized user may access and/or share ePHI if devices storing ePHI are allowed to be removed from your facility. Policies regarding the removal or movement of devices storing ePHI should be strictly enforced.

Some potential impacts include:

- Human threats, such as unauthorized or malicious users who can compromise the confidentiality, integrity, and availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) 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 address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.
[45 CFR §164.310(d)(2)(i)]

Establish guidelines for the removal of equipment and media for the maintenance or disposal of information. Your guidelines should include policies and procedures for sanitization of media where ePHI is stored.
[NIST SP 800-53 MP-6]

PH35 - §164.310(d)(2)(ii) Required Do you have procedures that describe how your practice should remove ePHI from its storage media/ electronic devices before the media is re-used?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

At times, storage media is re-used. For example, when one workforce member resigns, the USB, laptop, or tablet computer that was assigned to him/her might be reassigned to a different workforce member.

Consider the steps that your practice has taken to make sure that ePHI is removed from storage media before it is stored and is awaiting re-use by another workforce member.

Possible Threats and Vulnerabilities:

ePHI can be accessed by an unauthorized user, such as a new workforce member to whom the device is assigned, if you do not have policies and procedures that describe how to remove ePHI from electronic devices and media before they are stored awaiting re-use.

Some potential impacts include:

• Human threats, such as unauthorized or malicious users who can compromise the confidentiality, integrity, and availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
[45 CFR §164.310(d)(2)(ii)]

Establish a process for the sanitizing (removal) of ePHI from equipment and media where it is stored prior to preparing it for reuse.
[NIST SP 800-53 MP-6]

PH36 - §164.310(d)(2)(iii) Addressable Does your practice maintain a record of movements of hardware and media and the person responsible for the use and security of the devices or media containing ePHI outside the facility?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Have you taken steps to implement procedures to document the day-to-day location of information technology or storage media on which PHI is stored by your practice and the assignment of a staff member responsible for maintaining this record?

Possible Threats and Vulnerabilities:

ePHI can be subject to undiscovered incidents involving unauthorized access, theft, and loss if you do not maintain a record of hardware and electronic media movement outside the facility. As such, the ePHI can leave your facility without being monitored or traced.

Some potential impacts include:

• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Maintain a record of the movements of hardware and electronic media and any person responsible for the use and security of the devices and media containing ePHI outside the facility.
[45 CFR §164.310(d)(2)(iii)]

Develop a process for maintaining records of hardware and electronic media being transported to and from your facility, such as:

•Preparing and keeping an up-to-date component inventory of information systems that contain ePHI.
[NIST SP 800-53 CM-8]
•Requiring signed access agreements before enabling access to information systems that contain ePHI.
[NIST SP 800-53 PS-6]

PH37 - §164.310(d)(2)(iii) Addressable Do you maintain records of employees removing electronic devices and media from your facility that has or can be used to access 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:

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

Related Information:

Things to Consider to Help Answer the Question:

Employees might bring their own electronic devices and media to work. Other electronic devices and media might be issued to them by your practice. These devices and media can store significant amounts of ePHI that can leave the practice's facility without being noticed.

Consider the steps that your practice has taken to identify storage media/electronic devices that your workforce members, contractors, and visitors have when they enter and leave your facility.

Possible Threats and Vulnerabilities:

ePHI can leave your facility without being detected or traced if you do not keep records of the devices storing ePHI and/or the associated users entering and leaving your facility.

Some potential impacts include:

- Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Maintain a record of the movements of hardware and electronic media and any person responsible for it.
[45 CFR §164.310(d)(2)(iii)]

Establish policies and procedures for transportation of media where ePHI is stored. Include requiring the creation and maintenance of an inventory of electronic devices and media. Include the requirement to maintain a log of individuals that access or remove media.
[NIST SP 800-53 MP-5]

PH38 - §164.310(d)(2)(iv) Addressable Does your organization create backup files prior to the movement of equipment or media to ensure that data is available when it is needed?

○ 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:

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

Related Information:

Things to Consider to Help Answer the Question:

The availability of ePHI that is stored on an information system, a component, equipment, workstation, or other storage media can be compromised if the equipment is damaged, destroyed, or lost during transport.

Consider the steps that your practice has taken to make sure that it has an exact copy of the ePHI so that the information is available even if the equipment or storage media is lost, stolen, or destroyed during transport.

Possible Threats and Vulnerabilities:

ePHI can be lost, corrupted, or made inaccessible in the future if your practice does not create backup files that are retrievable and exact copies.

Some potential impacts include:

- Natural threats, such as hurricanes, tornadoes, snow, ice, floods, and earthquakes, which can cause damage to your facilities and media, resulting in loss of ePHI.
- Environmental threats, such as power failure and temperature extremes, which can cause damage to your media and information systems.
- Human threats, such as an unauthorized or malicious user who can vandalize or compromise the integrity, confidentiality, and availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:

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

Create a retrievable, exact copy of ePHI before the movement of equipment.
[45 CFR §164.310(d)(2)(iv)]

Develop a process for the movement of equipment or media. Include policies and procedures for:

- Backing up information systems where ePHI is stored.
[NIST SP 800-53 CP-9]
- Handling storage media where ePHI is stored.
[NIST SP 800-53 MP-4]