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: September 2016

DISCLAIMER

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

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology 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 within HHS
ONC	The Office of the National Coordinator for Health Information Technology within HHS
PHI	Protected Health Information
RBAC	Role-based Access Control
SRA	Security Risk Assessment
SRA Tool	Security Risk Assessment Tool
USB	Universal Serial Bus

How to Use this Document

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

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

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

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

	Likelihood			
Impact		Low	Medium	High
	Low	Low Risk	Low Risk	Low Risk
	Medium	Low Risk	Medium Risk	Medium Risk
	High	Low Risk	Medium Risk	High Risk

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

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

Why you should use this Tool?

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

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

These three goals: availability, confidentiality, and integrity are the reasons why appropriately securing ePHI for which you are responsible is legally required. Underneath these important concepts are the details of how effectively your policies, procedures, staff education, and security controls work. Using this tool will help you identify specific areas to focus your

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

attention in improving how you secure ePHI. While ONC does require that Certified EHR Technology have certain security features built in, for some of these features, you need to take advantage of them, sort of like a seat belt in a car: every car has seatbelts, but you need to buckle them. This tool will help you identify those areas where you need to "buckle up."

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:

A detailed list of all policies and procedures were supplied. After thorough review, we determine policies and procedures are sufficient.

Please include any additional notes:

Expectations are met. However, are passwords updated every 6 months or 3 months? There is conflicting information between interview with Mrs. Jones and Policies listed. Make sure all policies are consistent throughout where details can overlap and staff practices match.

Please detail your remediation plan:

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

○ Low

○ Medium

○ High

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

○ Low

○ Medium

○ High

Overall Security Risk:

○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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 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); and

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

Implement policies and procedures to 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:

Waverly has policies and procedures that govern annual risk assessment and ongoing assessment. This includes assessing potential risks with business associate agreements.

Please include any additional notes:

Expectations are met

Please detail your remediation plan:

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

○ Low

○ Medium

○ High

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

○ Low

○ Medium

○ High

Overall Security Risk:

○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Implement policies and procedures to 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:

We are a relatively small practice, while impact is not measured, any downtime makes a negative impact to processes.

Please include any additional notes:

N/A

Please detail your remediation plan:

Consider whether your practice categorizes its information systems as high, moderate, or low impact systems (that is, if your information systems were unavailable, would this have a high, moderate, or low impact on your daily operations?). Based on this information, strategize, and mitigate areas of concern with a moderate or large impact.

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Overall Security Risk:

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Risk analysis 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 (that is, if your information systems were unavailable, would this have a high, moderate, or low impact on your daily operations?).

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

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:

Waverly conducts an annual risk assessment and sharing the results with all staff to receive their input. They also audit access controls to software, hardware and physical building every 6 months. However, I could not find documentation where risk assessments are conducted upon occurrence of a significant event.

Please include any additional notes:

Although Waverly encrypts all data, they don't have the ability to determine if someone has intercepted our data while it is in transit.

Please detail your remediation plan:

Waverly is looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered or deleted. We also recommend adding to policies and procedures to do a risk analysis upon changes and any significant events.

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Overall Security Risk:

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Consider that 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:

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

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:

We know we have an unsecured fax machine that is connected to a telephone line. We have a policy for managing faxes, and we do not send anything out until we have received a confirmation fax from the intended recipient. We only receive some lab results from the imaging center. The fax machine is located in the central work area and is not accessible to the public. They are unsecured off hours and we have no way to lock them down after we leave. Lab data is received via and it sits in the fax machine were we pick it up in the morning. We lock down all workstations at the end of the day so cleaning staff cannot access any electronic information. We lock up all cabinets that contain PHI, such as charts, at the end of each day. We have a policy that describes who has access to data and where to get access, such as keys and log ins by staff.

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Overall Security Risk:

○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Implement security measures 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

Overall Security Risk:

- ○ 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:

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

Implement security measures 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

Overall Security Risk:

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

Implement security measures 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

Overall Security Risk:

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

Implement security measures 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

Implement procedures to 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

Overall Security Risk:

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

Implement procedures to 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

Overall Security Risk:

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

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

Overall Security Risk:

○ 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:

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

Implement policies and procedures to 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

Overall Security Risk:

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

Implement policies and procedures to 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

Overall Security Risk:

○ 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.

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

Implement policies and procedures to 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

Overall Security Risk:

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

Implement policies and procedures to 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

Overall Security Risk:

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

Implement policies and procedures to 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

Overall Security Risk:

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

Implement procedures 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

Overall Security Risk:

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

Implement procedures 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

Overall Security Risk:

- ○ 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.

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

Implement procedures 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

Overall Security Risk:

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

Implement procedures 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

Overall Security Risk:

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

Implement procedures to 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

Overall Security Risk:

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

Implement procedures to 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement policies and procedures 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

Overall Security Risk:

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

Implement a 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

Overall Security Risk:

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

Implement a 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

Overall Security Risk:

- ○ 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:

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

Implement a 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

Overall Security Risk:

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

Implement a 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

Overall Security Risk:

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

Implement a 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

Implement policies and procedures to 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

Establish (and implement as needed) 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

Overall Security Risk:

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

Establish (and implement as needed) 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

Overall Security Risk:

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

Establish (and implement as needed) 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

Overall Security Risk:

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

Establish and implement 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

Overall Security Risk:

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

Establish (and implement as needed) procedures 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

Overall Security Risk:

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

Establish (and implement as needed) procedures 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

Overall Security Risk:

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

Implement procedures 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

Implement 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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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

Overall Security Risk:

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

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]