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

Security Risk Assessment Tool
Physical Safeguards Content

Version Date: March 2014

DISCLAIMER

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

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

Contents

Acronym Index

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

Establish physical access control procedures to:

• Limit entrance to and exit of the facility using one or more physical access methods.
• Control access to areas within the facility that are designated as publicly accessible.
• Secure keys, combinations, and other physical access devices.
[NIST SP 800-53 PE-3]

Establish physical access authorization procedures to:

• Develop and maintain a list of individuals with authorized access to the facility.
• Issue authorization credentials.
[NIST SP 800-53 PE-2]

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

Establish and periodically test your emergency procedures to:

Establish an alternate processing site to continue operations by:

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

• Ensuring required equipment and supplies are onsite.
• Ensuring applicable security safeguards are in place.
[NIST SP 800-53 CP-7]

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

• Security controls.
• Continuous monitoring of control effectiveness.
• Incident reporting and response.
[NIST SP 800-53 PE-17]

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

○ Yes

○ No

If no, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

• Roles and responsibilities.
• Periodic review and updating.
• Timely communication and distribution to relevant workforce members.
[NIST SP 800-53 CP-2]

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

storage locations during a disaster.

Some potential impacts include:

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

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

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

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

Store a copy of ePHI at an alternative location:

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that the methods you rely on to protect your facilities are still effective after an employee, business associate, or service

provider transfers, quits, or is fired. Steps may include re-keying locks or changing combinations.

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

and performance of your practice's information systems.
• Human threats, such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

Examples of Safeguards:
Some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you may choose will depend on the degree of risk (likelihood) and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.
Establish policies and procedures to protect the facility and its equipment from unauthorized physical access, tampering, and theft.
[45 CFR §164.310(a)(2)(ii)]

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

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

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

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

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

• Policies and procedures for physical and environmental protection.

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

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

○ Yes

○ No

If no, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

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

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

Possible Threats and Vulnerabilities:

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

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

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

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

Have policies and procedures in place to:

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

Establish physical access control procedures to:

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

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

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

Possible Threats and Vulnerabilities:

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

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

○ Cost

○ Practice Size

- ○ Complexity
- ○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

Examples of Safeguards:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

Examples of Safeguards:

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

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or electronic device that can access ePHI (such as laptops, printers, copiers, tablets, smart phones, monitors, and other devices).
[45 CFR §164.310(b)]

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

procedures for:

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

Examples of Safeguards:

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

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

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

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

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

Possible Threats and Vulnerabilities:

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

Some potential impacts include:

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

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

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

Develop policies and procedures for acceptable use and storage of electronic devices that are remotely accessing ePHI.
[NIST SP 800-53 MP-4]

PH30 - §164.310(d)(1) Standard Does your practice have security policies and procedures to physically protect and securely store electronic devices and media inside your facility(ies) until they can be securely disposed of or destroyed?

○ Yes

○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Storage media and devices take on many different forms, from portable hard drives to thumb drives that fit easily onto a key ring. While small, these devices can hold enormous amounts of electronic data. Consider the policies and procedures put in place by your practice to securely store and track movement of devices and electronic media in your facilities from the time they are acquired to the time they are destroyed.

Possible Threats and Vulnerabilities:

ePHI can be removed from your facilities without being observed and/or monitored if your practice does not have security policies and procedures to physically protect and securely store electronic devices and media.

Some potential impacts include:

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

Examples of Safeguards:

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

Implement policies and procedures that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop a security policy for the protection and storage of your digital media, including a documented component inventory of information systems that contain ePHI [NIST SP 800-53 CM-8] and policies and procedures for:

• Storing media where ePHI is stored.
[NIST SP 800-53 MP-4]
• Protecting media that contain ePHI.
[NIST SP 800-53 MP-1]

• Accessing media that contain ePHI.
[NIST SP 800-53 MP-2]
• Marking the media where ePHI is stored.
[NIST SP 800-53 MP-3]

PH31 - §164.310(d)(1) Standard Do you remove or destroy ePHI from information technology devices and media prior to disposal of the device?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

Consider the steps that your practice takes to make sure that the ePHI stored on electronic devices and media is deleted prior to disposal of the device.

Possible Threats and Vulnerabilities:

ePHI left in discarded devices and media can be accessed by malicious unauthorized users if you do not sanitize (remove) that information prior to disposal or destruction of the equipment.

Some potential impacts include:

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

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

Implement policies and procedures that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop a process for sanitizing and securely disposing of electronic devices and media that contain ePHI.
[NIST SP 800-53 MP-6]

PH32 - §164.310(d)(1) Standard Do you maintain records of the movement of electronic devices and media inside your facility?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Electronic devices and storage media can store vast amounts of ePHI. Consider the steps that your practice takes to make sure it knows where electronic devices and storage media are on a day-to-day basis, especially when they are moved internally within your practice area.

Possible Threats and Vulnerabilities:

You cannot effectively apply the policies designed to protect the confidentiality, integrity, and availability of ePHI if you do not maintain an inventory of what ePHI you maintain and where it resides (e.g., on electronic devices and media).

Some potential impacts include:

• Natural threats, such as hurricanes, tornadoes, snow, ice, floods, and earthquakes, which can cause damage to your facilities, resulting in loss of ePHI.
• Environmental threats, such as power failure and temperature extremes, which can cause damage to your information systems.
• Human threats, such as an unauthorized user who can vandalize or compromise the confidentiality, integrity, or availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Implement policies and procedures that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

Develop and maintain an inventory of your storage media and/or information systems that handle ePHI. As part of your security plan for handling storage media, include policies and procedures for transportation of media where ePHI is stored.
[NIST SP 800-53 MP-5]

PH33 - §164.310(d)(1) Standard Have you developed and implemented policies and procedures that specify how your practice should dispose of electronic devices and media containing ePHI?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

Electronic devices and media can contain significant amounts of ePHI, and secure disposal is very important. Consider the steps that your practice has taken to make sure that its electronic devices and media are disposed of in a manner that makes sure the confidentiality of ePHI is not compromised.

Possible Threats and Vulnerabilities:

ePHI can leave your facility and be accessed by an unauthorized user without your knowledge if you do not have policies and procedures in place that define how to properly sanitize and dispose of electronic devices and media. A malicious user can then use undeleted utilities to recover data from discarded media.

Some potential impacts include:

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

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

Implement policies and procedures that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
[45 CFR §164.310(d)(1)]

As part of your plan for disposing of electronic devices and media containing ePHI, include policies and procedures for the sanitization of media where ePHI is stored.
[NIST SP 800-53 MP-6]

PH34 - §164.310(d)(2)(i) Required Do you require that all ePHI is removed from equipment and media before you remove the equipment or media from your facilities for offsite maintenance or disposal?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

ePHI can be stored in photo copiers, smart phones, tablets, laptops, and a wide array of electronic devices and media. In some instances, it may not be readily apparent to the user that ePHI is there. Consider the steps that your practice has taken to make sure that its ePHI is identified and removed from equipment, workstations, and information systems before they are removed from the facility for maintenance or disposal.

Possible Threats and Vulnerabilities:

An unauthorized user may access and/or share ePHI if devices storing ePHI are allowed to be removed from your facility. Policies regarding the removal or movement of devices storing ePHI

should be strictly enforced.

Some potential impacts include:

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

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

Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.
[45 CFR §164.310(d)(2)(i)]

Establish guidelines for the removal of equipment and media for the maintenance or disposal of information. Your guidelines should include policies and procedures for sanitization of media where ePHI is stored.
[NIST SP 800-53 MP-6]

PH35 - §164.310(d)(2)(ii) Required Do you have procedures that describe how your practice should remove ePHI from its storage media/ electronic devices before the media is re-used?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low

○ Medium

○ High

Related Information:

Things to Consider to Help Answer the Question:

At times, storage media is re-used. For example, when one workforce member resigns, the USB, laptop, or tablet computer that was assigned to him/her might be reassigned to a different workforce member.

Consider the steps that your practice has taken to make sure that ePHI is removed from storage media before it is stored and is awaiting re-use by another workforce member.

Possible Threats and Vulnerabilities:

ePHI can be accessed by an unauthorized user, such as a new workforce member to whom the device is assigned, if you do not have policies and procedures that describe how to remove ePHI from electronic devices and media before they are stored awaiting re-use.

Some potential impacts include:

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

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

Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
[45 CFR §164.310(d)(2)(ii)]

Establish a process for the sanitizing (removal) of ePHI from equipment and media where it is stored prior to preparing it for reuse.
[NIST SP 800-53 MP-6]

PH36 - §164.310(d)(2)(iii) Addressable Does your practice maintain a record of movements of hardware and media and the person responsible for the use and security of the devices or media containing ePHI outside the facility?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Have you taken steps to implement procedures to document the day-to-day location of information technology or storage media on which PHI is stored by your practice and the assignment of a staff member responsible for maintaining this record?

Possible Threats and Vulnerabilities:

ePHI can be subject to undiscovered incidents involving unauthorized access, theft, and loss if you do not maintain a record of hardware and electronic media movement outside the facility. As such, the ePHI can leave your facility without being monitored or traced.

Some potential impacts include:

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

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

Maintain a record of the movements of hardware and electronic media and any person responsible for the use and security of the devices and media containing ePHI outside the facility.
[45 CFR §164.310(d)(2)(iii)]

Develop a process for maintaining records of hardware and electronic media being transported to and from your facility, such as:

•Preparing and keeping an up-to-date component inventory of information systems that contain ePHI.
[NIST SP 800-53 CM-8]
•Requiring signed access agreements before enabling access to information systems that contain ePHI.
[NIST SP 800-53 PS-6]

PH37 - §164.310(d)(2)(iii) Addressable Do you maintain records of employees removing electronic devices and media from your facility that has or can be used to access ePHI?

○ Yes

○ No

If no, please select from the following:

○ Cost

○ Practice Size

○ Complexity

○ Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

○ Low

○ Medium

○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

Employees might bring their own electronic devices and media to work. Other electronic devices and media might be issued to them by your practice. These devices and media can store significant amounts of ePHI that can leave the practice's facility without being noticed.

Consider the steps that your practice has taken to identify storage media/electronic devices that your workforce members, contractors, and visitors have when they enter and leave your facility.

Possible Threats and Vulnerabilities:

ePHI can leave your facility without being detected or traced if you do not keep records of the devices storing ePHI and/or the associated users entering and leaving your facility.

Some potential impacts include:

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

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

Maintain a record of the movements of hardware and electronic media and any person responsible for it.
[45 CFR §164.310(d)(2)(iii)]

Establish policies and procedures for transportation of media where ePHI is stored. Include requiring the creation and maintenance of an inventory of electronic devices and media. Include the requirement to maintain a log of individuals that access or remove media. [NIST SP 800-53 MP-5]

PH38 - §164.310(d)(2)(iv) Addressable Does your organization create backup files prior to the movement of equipment or media to ensure that data is available when it is needed?

- ○ Yes
- ○ No

If no, please select from the following:

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

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

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

- ○ Low
- ○ Medium
- ○ High

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

- ○ Low
- ○ Medium
- ○ High

Related Information:

Things to Consider to Help Answer the Question:

The availability of ePHI that is stored on an information system, a component, equipment, workstation, or other storage media can be compromised if the equipment is damaged, destroyed, or lost during transport.

Consider the steps that your practice has taken to make sure that it has an exact copy of the ePHI so that the information is available even if the equipment or storage media is lost, stolen, or destroyed during transport.

Possible Threats and Vulnerabilities:

ePHI can be lost, corrupted, or made inaccessible in the future if your practice does not create backup files that are retrievable and exact copies.

Some potential impacts include:

• Natural threats, such as hurricanes, tornadoes, snow, ice, floods, and earthquakes, which can cause damage to your facilities and media, resulting in loss of ePHI.
• Environmental threats, such as power failure and temperature extremes, which can cause damage to your media and information systems.
• Human threats, such as an unauthorized or malicious user who can vandalize or compromise the integrity, confidentiality, and availability of ePHI. Unauthorized disclosure, loss, or theft of ePHI can lead to identity theft.

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

Create a retrievable, exact copy of ePHI before the movement of equipment.
[45 CFR §164.310(d)(2)(iv)]

Develop a process for the movement of equipment or media. Include policies and procedures for:

• Backing up information systems where ePHI is stored.
[NIST SP 800-53 CP-9]
• Handling storage media where ePHI is stored.
[NIST SP 800-53 MP-4]