****

|  |
| --- |
| **U.S. Department of Health and Human Services (HHS)**  **The Office of the National Coordinator for Health Information Technology (ONC)**  **Security Risk Assessment (SRA) Tool**  **Administrative Safeguards Content** |
| **Version Date: September 2016** |
|  |
| **DISCLAIMER**  The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with Federal, State, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights (OCR) Health Information Privacy website at: [www.hhs.gov/ocr/privacy/hipaa/understanding/index.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html)  NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional’s specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this tool. |

**Contents**

[**Acronym Index** viii](#_Toc459304801)

[**How to Use this Document** 9](#_Toc459304802)

[**A1 - §164.308(a)(1)(i) Standard** Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)? 12](#_Toc459304803)

[**A2 - §164.308(a)(1)(i) Standard** Does your practice have a process for periodically reviewing its risk analysis policies and procedures and making updates as necessary? 14](#_Toc459304804)

[**A3 - §164.308(a)(1)(ii)(A) Required** Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable? 17](#_Toc459304805)

[**A4 - §164.308(a)(1)(ii)(A) Required** Does your practice periodically complete an accurate and thorough risk analysis, such as upon occurrence of a significant event or change in your business organization or environment? 20](#_Toc459304806)

[**A5 - §164.308(a)(1)(ii)(B) Required** Does your practice have a formal documented program to mitigate the threats and vulnerabilities to ePHI identified through the risk analysis? 22](#_Toc459304807)

[**A6 - §164.308(a)(1)(ii)(B) Required** Does your practice assure that its risk management program prevents against the impermissible use and disclosure of ePHI. 25](#_Toc459304808)

[**A7 - §164.308(a)(1)(ii)(B) Required** Does your practice document the results of its risk analysis and assure the results are distributed to appropriate members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified through the risk analysis? 27](#_Toc459304809)

[**A8 - §164.308(a)(1)(ii)(B) Required** Does your practice formally document a security plan? 29](#_Toc459304810)

[**A9 - §164.308(a)(1)(ii)(C) Required** Does your practice have a formal and documented process or regular human resources policy to discipline workforce members who have access to your organization’s ePHI if they are found to have violated the office’s policies to prevent system misuse, abuse, and any harmful activities that involve your practice's ePHI? 32](#_Toc459304811)

[**A10 - §164.308(a)(1)(ii)(C) Required** Does your practice include its sanction policies and procedures as part of its security awareness and training program for all workforce members? 35](#_Toc459304812)

[**A11 - §164.308(a)(1)(ii)(D) Required** Does your practice have policies and procedures for the review of information system activity? 37](#_Toc459304813)

[**A12 - §164.308(a)(1)(ii)(D) Required** Does your practice regularly review information system activity? 40](#_Toc459304814)

[**A13 - §164.308(a)(2) Required** Does your practice have a senior-level person whose job it is to develop and implement security policies and procedures or act as a security point of contact? 42](#_Toc459304815)

[**A14 - §164.308(a)(2) Required** Is your practice’s security point of contact qualified to assess its security protections as well as serve as the point of contact for security policies, procedures, monitoring, and training? 45](#_Toc459304816)

[**A15 - §164.308(a)(2) Required** Does your practice have a job description for its security point of contact that includes that person's duties, authority, and accountability? 47](#_Toc459304817)

[**A16 - §164.308(a)(2) Required** Does your practice make sure that its workforce members and others with authorized access to your ePHI know the name and contact information for its security point of contact and know to contact this person if there are any security problems? 50](#_Toc459304818)

[**A17 - §164.308(a)(3)(i) Required** Does your practice have a list that includes all members of its workforce, the roles assigned to each, and the corresponding access that each role enables for your practice’s facilities, information systems, electronic devices, and ePHI? 52](#_Toc459304819)

[**A18 - §164.308(a)(3)(i) Required** Does your practice know all business associates and the access that each requires for your practice’s facilities, information systems, electronic devices, and ePHI? 55](#_Toc459304820)

[**A19 - §164.308(a)(3)(i) Required** Does your practice clearly define roles and responsibilities along logical lines and assures that no one person has too much authority for determining who can access your practice's facilities, information systems, and ePHI? 58](#_Toc459304821)

[**A20 - §164.308(a)(3)(i) Required** Does your practice have policies and procedures that make sure those who need access to ePHI have access and those who do not are denied such access? 61](#_Toc459304822)

[**A21 - §164.308(a)(3)(i) Required** Has your practice chosen someone whose job duty is to decide who can access ePHI (and under what conditions) and to create ePHI access rules that others can follow? 64](#_Toc459304823)

[**A22 - §164.308(a)(3)(ii)(A) Addressable** Does your practice define roles and job duties for all job functions and keep written job descriptions that clearly set forth the qualifications? 66](#_Toc459304824)

[**A23 - §164.308(a)(3)(ii)(A) Addressable** Does your practice have policies and procedures for access authorization that support segregation of duties? 69](#_Toc459304825)

[**A24 - §164.308(a)(3)(ii)(A) Addressable** Does your practice implement procedures for authorizing users and changing authorization permissions? 72](#_Toc459304826)

[**A25 - §164.308(a)(3)(ii)(A) Addressable** Do your practice’s policies and procedures for access authorization address the needs of those who are not members of its workforce? 74](#_Toc459304827)

[**A26 - §164.308(a)(3)(ii)(B) Addressable** Does your organization have policies and procedures that authorize members of your workforce to have access to ePHI and describe the types of access that are permitted? 77](#_Toc459304828)

[**A27 - §164.308(a)(3)(ii)(B) Addressable** Do your practice’s policies and procedures require screening workforce members prior to enabling access to its facilities, information systems, and ePHI to verify that users are trustworthy? 80](#_Toc459304829)

[**A28 - §164.308(a)(3)(ii)(C) Addressable** Does your practice have policies and procedures for terminating authorized access to its facilities, information systems, and ePHI once the need for access no longer exists? 82](#_Toc459304830)

[**A29 - §164.308(a)(3)(ii)(C) Addressable** Does your practice have formal policies and policies and procedures to support when a workforce member’s employment is terminated and/or a relationship with a business associate is terminated? 85](#_Toc459304831)

[**A30 - §164.308(a)(4)(i) Standard** Do your practice’s policies and procedures describe the methods it uses to limit access to its ePHI? 88](#_Toc459304832)

[**A31 - §164.308(a)(4)(ii)(B)** Does your practice have policies and procedures that explain how it grants access to ePHI to its workforce members and to other entities (business associates)? 91](#_Toc459304833)

[**A32 - §164.308(a)(4)(ii)(C) Addressable** Do the roles and responsibilities assigned to your practice’s workforce members support and enforce segregation of duties? 94](#_Toc459304834)

[**A33 - §164.308(a)(4)(ii)(C) Addressable** Does your practice’s policies and procedures explain how your practice assigns user authorizations (privileges), including the access that are permitted? 97](#_Toc459304835)

[**A34 - §164.308(a)(5)(i) Standard** Does your practice have a training program that makes each individual with access to ePHI aware of security measures to reduce the risk of improper access, uses, and disclosures? 99](#_Toc459304836)

[**A35 - §164.308(a)(5)(i) Standard** Does your practice periodically review and update its security awareness and training program in response to changes in your organization, facilities or environment? 102](#_Toc459304837)

[**A36 - §164.308(a)(5)(i) Standard** Does your practice provide ongoing basic security awareness to all workforce members, including physicians? 104](#_Toc459304838)

[**A37 - §164.308(a)(5)(i) Standard** Does your practice provide role-based training to all new workforce members? 107](#_Toc459304839)

[**A38 - §164.308(a)(5)(i) Standard** Does your practice keep records that detail when each workforce member satisfactorily completed periodic training? 110](#_Toc459304840)

[**A39 - §164.308(a)(5)(ii)(A) Addressable** As part of your practice’s ongoing security awareness activities, does your practice prepare and communicate periodic security reminders to communicate about new or important issues? 112](#_Toc459304841)

[**A40 - §164.308(a)(5)(ii)(B) Addressable** Does your practice’s awareness and training content include information about the importance of implementing software patches and updating antivirus software when requested? 115](#_Toc459304842)

[**A41 - §164.308(a)(5)(ii)(B) Addressable** Does your practice’s awareness and training content include information about how malware can get into your systems? 117](#_Toc459304843)

[**A42 - §164.308(a)(5)(ii)(C) Addressable** Does your practice include log-in monitoring as part of its awareness and training programs? 120](#_Toc459304844)

[**A43 - §164.308(a)(5)(ii)(D) Addressable** Does your practice include password management as part of its awareness and training programs? 122](#_Toc459304845)

[**A44 - §164.308(a)(6)(i) Standard** Does your practice have policies and procedures designed to help prevent, detect and respond to security incidents? 125](#_Toc459304846)

[**A45 - §164.308(a)(6)(ii) Required** Does your practice have incident response policies and procedures that assign roles and responsibilities for incident response? 128](#_Toc459304847)

[**A46 - §164.308(a)(6)(ii) Required** Does your practice identify members of its incident response team and assure workforce members are trained and that incident response plans are tested? 130](#_Toc459304848)

[**A47 - §164.308(a)(6)(ii) Required** Does your practice’s incident response plan align with its emergency operations and contingency plan, especially when it comes to prioritizing system recovery actions or events to restore key processes, systems, applications, electronic device and media, and information (such as ePHI)? 133](#_Toc459304849)

[**A48 - §164.308(a)(6)(ii) Required** Does your practice implement the information system’s security protection tools to protect against malware? 135](#_Toc459304850)

[**A49 - §164.308(a)(7)(i) Standard** Does your practice know what critical services and ePHI it must have available to support decision making about a patient’s treatment during an emergency? 138](#_Toc459304851)

[**A50 - §164.308(a)(7)(i) Standard** Does your practice consider how natural or man-made disasters could damage its information systems or prevent access to ePHI and develop policies and procedures for responding to such a situation? 140](#_Toc459304852)

[**A51 - §164.308(a)(7)(i) Standard** Does your practice regularly review/update its contingency plan as appropriate? 143](#_Toc459304853)

[**A52 - §164.308(a)(7)(ii)(A) Required** Does your practice have policies and procedures for the creation and secure storage of an electronic copy of ePHI that would be used in the case of system breakdown or disaster? 146](#_Toc459304854)

[**A53 - §164.308(a)(7)(ii)(B) Required** Does your practice have policies and procedures for contingency plans to provide access to ePHI to continue operations after a natural or human-made disaster? 149](#_Toc459304855)

[**A54 - §164.308(a)(7)(ii)(C) Required** Does your practice have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of ePHI immediately after a crisis situation? 151](#_Toc459304856)

[**A55 - §164.308(a)(7)(ii)(D) Addressable** Does your practice have policies and procedures for testing its contingency plans on a periodic basis? 154](#_Toc459304857)

[**A56 - §164.308(a)(7)(ii)(E) Addressable** Does your practice implement procedures for identifying and assessing the criticality of its information system applications and the storage of data containing ePHI that would be accessed through the implementation of its contingency plans? 157](#_Toc459304858)

[**A57 - §164.308(a)(8) Standard** Does your practice maintain and implement policies and procedures for assessing risk to ePHI and engaging in a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of your practice’s ePHI? 160](#_Toc459304859)

[**A58 - §164.308(a)(8) Standard** Does your practice periodically monitor its physical environment, business operations, and information system to gauge the effectiveness of security safeguards? 162](#_Toc459304860)

[**A59 - §164.308(a)(8) Standard** Does your practice identify the role responsible and accountable for assessing risk and engaging in ongoing evaluation, monitoring, and reporting? 165](#_Toc459304861)

[**A60 - §164.308(b)(1) Standard** Does your practice identify the role responsible and accountable for making sure that business associate agreements are in place before your practice enables a service provider to begin to create, access, store or transmit ePHI on your behalf? 168](#_Toc459304862)

[**A61 - §164.308(b)(1) Standard** Does your practice maintain a list of all of its service providers, indicating which have access to your practice’s facilities, information systems and ePHI? 171](#_Toc459304863)

[**A62 - §164.308(b)(1) Standard** Does your practice have policies and implement procedures to assure it obtains business associate agreements? 173](#_Toc459304864)

[**A63 - §164.308(b)(2) Required** If your practice is the business associate of another covered entity and your practice has subcontractors performing activities to help carry out the activities that you have agreed to carry out for the other covered entity that involve ePHI, does your practice require these subcontractors to provide satisfactory assurances for the protection of the ePHI? 176](#_Toc459304865)

[**A64 - §164.308(b)(3) Required** Does your practice execute business associate agreements when it has a contractor creating, transmitting or storing ePHI? 178](#_Toc459304866)

[**O1 - §164.314(a)(1)(i) Standard** Does your practice assure that its business associate agreements include satisfactory assurances for safeguarding ePHI? 181](#_Toc459304867)

[**O2 - §164.314(a)(2)(i) Required** Do the terms and conditions of your practice’s business associate agreements state that the business associate will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the practice and timely report security incidents to your practice? 184](#_Toc459304868)

[**O3 - §164.314(a)(2)(iii) Required** If your practice is the business associate of a covered entity do the terms and conditions of your practice’s business associate agreements state that your subcontractor (business associate) will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the covered entity? 187](#_Toc459304869)

[**PO1 -§164.316(a) Standard** Do your practice’s processes enable the development and maintenance of policies and procedures that implement risk analysis, informed risk-based decision making for security risk mitigation, and effective mitigation and monitoring that protects the privacy, confidentiality, integrity, and availability of ePHI? 190](#_Toc459304870)

[**PO2 - §164.316(b)(1)(i) Standard** Does your practice assure that its policies and procedures are maintained in a manner consistent with other business records? 193](#_Toc459304871)

[**PO3 - §164.316(b)(1)(ii) Standard** Does your practice assure that its other security program documentation is maintained in written manuals or in electronic form? 195](#_Toc459304872)

[**PO4 - §164.316(b)(2)(i) Required** Does your practice assure that its policies, procedures, and other security program documentation are retained for at least six (6) years from the date when it was created or last in effect, whichever is longer? 198](#_Toc459304873)

[**PO5 - §164.316(b)(2)(ii) Required** Does your practice assure that its policies, procedures and other security program documentation are available to those who need it to perform the responsibilities associated with their role? 200](#_Toc459304874)

[**PO6 - §164.316(b)(2)(iii) Required** Does your practice assure that it periodically reviews and updates (when needed) its policies, procedures, and other security program documentation? 203](#_Toc459304875)

# **Acronym Index**

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

**How to Use this Document**

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

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

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

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

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

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

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

**Why you should use this Tool?**

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

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

These three goals: availability, confidentiality, and integrity are the reasons why appropriately securing ePHI for which you are responsible is legally required. Underneath these important concepts are the details of how effectively your policies, procedures, staff education, and security controls work. Using this tool will help you identify specific areas to focus your attention in improving how you secure ePHI. While ONC does require that Certified EHR Technology have certain security features built in, for some of these features, you need to take advantage of them, sort of like a seat belt in a car: every car has seatbelts, but you need to buckle them. This tool will help you identify those areas where you need to “buckle up.”

# **A1 - §164.308(a)(1)(i) Standard** Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)?

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we maintain and distribute these policies on an internal repository that is regularly reviewed with employees. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

Consider whether your practice has an inventory that includes:

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

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

*Possible Threats and Vulnerabilities:*

Your practice may not have adequate controls to safeguard ePHI if it does not develop and implement policies and procedures for assessing and managing risk to its ePHI.

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to prevent, detect, contain, and correct security violations.

[45 CFR §164.308(a)(1)(i)]

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

[NIST SP 800-53 RA-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we review and update our policies on an annual basis, detailed in our Policy Management Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to prevent, detect, contain, and correct security violations.

[45 CFR §164.308(a)(1)(i)]

Review and update the current risk assessment policy and procedures to adapt your security program to changing needs.

[NIST SP 800-53 RA-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, our information architecture is comprised of:   1. Client Server 2. Machine Server 3. Database 4. Pillboxes   Our first priority is patient functionality should not be interrupted. To accommodate this, we design the system so that the pillbox is able to operate independent of a connection to any of the other elements. The pillboxes do not have access to ePHI, so this service would not compromise any PHI.  From a user perspective, the next most critical infrastructure element is the client server, as it’s the access point for health coaches to follow up with patients. We monitor uptime and disk utilization closely with this system and have procedures in place to spin up a new server rapidly to minimize any uptime.  The next most critical piece is the database, followed by the machine server. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Consider whether your practice categorizes its information systems as high, moderate, or low impact systems (that is, if your information systems were unavailable, would this have a high, moderate, or low impact on your daily operations?).

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

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

Consider whether your practice’s risk analysis:

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

[45 CFR §164.308(a)(1)(ii)(A)]

Categorize information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

[NIST SP 800-53 RA-2]

Document the security categorization results (including supporting rationale) in the security plan for the information system.

[NIST SP 800-53 RA-2]

Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official’s designated representative.

[NIST SP 800-53 RA-2]

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

* Yes
* **No**

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Risk analysis is done on an annual basis and during major product development phases. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
| We should conduct risk assessments after:   * Major security incidents * Large customer partnerships constituting order of magnitude changes in scale * Any doubling of firm size * Major software update to fundamental information systems used |

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

* **Low**
* Medium
* High

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

* Low
* **Medium**
* High

**Overall Security Risk:**

* Low
* **Medium**
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that a significant event might be:

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

[45 CFR §164.308(a)(1)(ii)(A)]

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| The plan is detailed below and can be found in the Risk Management Policy.  \* Step 1. Prioritize Actions  \* Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources  \* Output – Actions ranked from high to low  \* Step 2. Evaluate Recommended Control Options  \* Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.  \* Output – list of feasible controls  \* Step 3. Conduct Cost-Benefit Analysis  \* Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.  \* Output – Documented cost-benefit analysis of either implementing or not implementing each specific control  \* Step 4. Select Control(s)  \* Taking into account the information and results from previous steps, TowerView Health’s mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.  \* Output – Selected control(s)  \* Step 5. Assign Responsibility  \* Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.  \* Output – List of resources, responsible persons and their assignments  \* Step 6. Develop Safeguard Implementation Plan  \* Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:  \* Each risk or vulnerability/threat pair and risk level;  \* Prioritized actions;  \* The recommended feasible control(s) for each identified risk;  \* Required resources for implementation of selected controls;  \* Team member responsible for implementation of each control;  \* Start date for implementation  \* Target date for completion of implementation;  \* Maintenance requirements.  \* The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals’ time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to TowerView Health Senior Management.  \* Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.  \* Output – Safeguard Implementation Plan  \* Step 7. Implement Selected Controls  \* As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.  \* Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.  \* Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.  \* If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.  \* Output – Residual Risk documentation |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice’s ePHI.
* Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
* Accurate ePHI might not be available, which can adversely impact your healthcare professionals’ ability to diagnose and treat the patient.

*Examples of Safeguards:*

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

[45 CFR §164.308(a)(1)(ii)(B)]

Document within a security plan the controls and methods in place or planned to mitigate the threats and vulnerabilities to ePHI identified as a result of conducting a risk analysis.

[NIST SP 800-53 PL-2]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Our risk management program reviews our Access Policy, our Audit Policy and our Data Integrity policy to prevent against impermissible use and disclosure of ePHI. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

Your practice may not be able protect and secure ePHI if it does not assure that its risk management program prevents against the impermissible use and disclosure of ePHI.

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

[45 CFR §164.308(a)(1)(ii)(B)]

Have a security plan that documents security safeguards and methods in place or planned to mitigate the threats and vulnerabilities to ePHI that are identified as a result of conducting a risk analysis.

[NIST SP 800-53 PL-2]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| \* Step 6. Develop Safeguard Implementation Plan  \* Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:  \* Each risk or vulnerability/threat pair and risk level;  \* Prioritized actions;  \* The recommended feasible control(s) for each identified risk;  \* Required resources for implementation of selected controls;  \* Team member responsible for implementation of each control;  \* Start date for implementation  \* Target date for completion of implementation;  \* Maintenance requirements.  \* The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals’ time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to TowerView Health Senior Management.  \* Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.  \* Output – Safeguard Implementation Plan  \* Step 7. Implement Selected Controls  \* As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.  \* Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.  \* Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.  \* If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.  \* Output – Residual Risk documentation |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice documents:

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

*Possible Threats and Vulnerabilities:*

Your practice may not be able to implement effective safeguards to protect ePHI if it does not document and share the results of your risk analysis with the staff responsible for making risk management decisions, developing risk-related policies, and implementing risk mitigation safeguards for ePHI.  
  
Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

[45 CFR §164.308(a)(1)(ii)(B)]

Document, review, and disseminate risk assessment results to members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified as a result of a risk assessment.

[NIST SP 800-53 RA-3]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Our security plan is formally documented in our internal procedures. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

[45 CFR §164.308(a)(1)(ii)(B)]

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

[NIST SP 800-53 PL-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| All workforce members report non-compliance of TowerView Health’s policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.  1. The Security Officer promptly facilitates a thorough investigation of all reported violations of TowerView Health’s security policies and procedures. The Security Officer may request assistance from others.  1. Complete an audit trail/log to identify and verify the violation and sequence of events.  2. Interview any individual that may be aware of or involved in the incident.  3. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.  4. Provide individuals suspected of non-compliance of the Security rule and/or TowerView Health’s policies and procedures the opportunity to explain their actions.  5. The investigators thoroughly documents the investigation as the investigation occurs.  2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.  3. A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member from TowerView Health.  4. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).  5. In the case of an insider threat, the Security Officer and Privacy Officer are to setup a team to investigate and mitigate the risk of insider malicious activity. TowerView Health workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.  6. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* **Medium**
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

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

*Possible Threats and Vulnerabilities:*

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

*Examples of Safeguards:*

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

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

Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures. The process should involve documenting when a formal employee sanctions process is initiated to include identifying the individual sanctioned and the associated reason.

[NIST SP 800-53 PS-8]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| All workforce members report non-compliance of TowerView Health’s policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.  1. The Security Officer promptly facilitates a thorough investigation of all reported violations of TowerView Health’s security policies and procedures. The Security Officer may request assistance from others.  1. Complete an audit trail/log to identify and verify the violation and sequence of events.  2. Interview any individual that may be aware of or involved in the incident.  3. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.  4. Provide individuals suspected of non-compliance of the Security rule and/or TowerView Health’s policies and procedures the opportunity to explain their actions.  5. The investigators thoroughly documents the investigation as the investigation occurs.  2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.  3. A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member from TowerView Health.  4. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).  5. In the case of an insider threat, the Security Officer and Privacy Officer are to setup a team to investigate and mitigate the risk of insider malicious activity. TowerView Health workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.  6. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Policies and procedures for system activity are detailed in the Audit Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Consider whether your practice:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Information system activity is reviewed by the Security Officer weekly. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

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

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

[NIST SP 800-53 AU-7]

Monitor information systems to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections. Deploy monitoring devices to identify unauthorized use of information systems.

[NIST SP 800-53 SI-4]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, the TowerView Health Security Officer is Hareesh Ganesan. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Consider that security includes responsibility for:

* Workforce security
* Vendor management
* Facility security
* Information system security

*Possible Threats and Vulnerabilities:*

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

*Examples of Safeguards:*

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

[45 CFR §164.308(a)(2)]

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

[NIST SP 800-53 CA-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| The Security Officer has thoroughly researched and reviewed both proper security protocols for HIPAA as well as best practices for web application development. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
| Utilizing further third party audits to ensure HIPAA compliance can help mitigate any additional gaps in knowledge necessary. |

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

* **Low**
* Medium
* High

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

* Low
* **Medium**
* High

**Overall Security Risk:**

* Low
* **Medium**
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

[45 CFR §164.308(a)(2)]

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

[NIST SP 800-53 CA-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Security officer roles and responsibilities are described in the TowerView Health Security Policies. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

*Examples of Safeguards:*

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

[45 CFR §164.308(a)(2)]

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

[NIST SP 800-53 CA-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| All employees are made aware in security awareness training of the contact information for the security point of contact. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

[45 CFR §164.308(a)(2)]

Provide incident response training to workforce members consistent with assigned roles and responsibilities.

[NIST SP 800-53 IR-2]

Require workforce members to report suspected security incidents and/or problems to your practice’s assigned security point of contact.

[NIST SP 800-53 IR-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| An up to date employee directory with access controls enabled is maintained internally. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.  
[45 CFR §164.308(a)(3)(i)]

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

[NIST SP 800-53 AC-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| A list of all access enabled for each business associate is maintained in a Google Docs spreadsheet. Access is reviewed regularly and policies for data destruction upon employee termination are specified. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.  
[45 CFR §164.308(a)(3)(i)]

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

[NIST SP 800-53 AC-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Roles and responsibilities are defined along logical lines to split up authority. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

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

*Examples of Safeguards:*

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

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.  
[45 CFR §164.308(a)(3)(i)]

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

[NIST SP 800-53 CA-6]

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

[NIST SP 800-53 AC-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we maintain a Systems Access Policy detailing ePHI access requirement principles. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.  
[45 CFR §164.308(a)(3)(i)]

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

[NIST SP 800-53 AC-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We currently designate rollout administrators who have strict access rules for PHI per rollout and define access rules for other users. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* Low
* Medium
* **High**

**Overall Security Risk:**

* Low
* **Medium**
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Human threats, such as a workforce member or service provider with excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.
* Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
* Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals’ ability to diagnose and treat their patients.

*Examples of Safeguards:*

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

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.  
[45 CFR §164.308(a)(3)(i)]

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

[NIST SP 800-53 AC-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we maintain roles and responsibilities for job descriptions. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Workforce members may not be held accountable for your practice’s overall security program.
* Human threats, such as a workforce member or service provider with excessive access privileges, can compromise the privacy, confidentiality, integrity or availability of ePHI.
* Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
* Accurate ePHI may not be timely available, which can adversely impact your healthcare professionals’ ability to diagnose and treat the patient.

*Examples of Safeguards:*

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

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

[45 CFR §164.308(a)(3)(ii)(A)]

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

[NIST SP 800-53 AC-1]

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

[NIST SP 800-53 PS-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We separate access privileges designation along distinct logical lines to ensure that chain of command does not interfere with access violations. All PHI access is defined based on roles rather than individuals to further secure access.  We separate logical access into:  Care coordinators: Access to adherence dashboard for authorized patients  Pharmacist: Access to medication schedule for authorized patients  Rollout Admin: Ability to assign users to a care coordinator within a given rollout  TVH Admin: Privileges to assign rollout administrator access for multiple rollouts  System Admin: Access to production database |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

[45 CFR §164.308(a)(3)(ii)(A)]

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

[NIST SP 800-53 AC-1]

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

Develop processes that implement security safeguards that restrict access to digital or non-digital media containing ePHI.

[NIST SP 800-53 MP-2]























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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, this is detailed in the Systems Access Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* Low
* **Medium**
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Examples of least privileges and minimum necessary access questions are:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

[45 CFR §164.308(a)(3)(ii)(B)]

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

[NIST SP 800-53 PS-1]

Establish processes to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and periodically review and update the signed access agreements.

[NIST SP 800-53 PS-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| \* The level of security assigned to a user to the organization’s information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.  \* All access requests are treated on a ‘least-access principle”.  \* TowerView Health maintains a minimum necessary approach to access to Customer data. As such, TowerView Health, including all workforce members, does not readily have access to any ePHI. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

[45 CFR §164.308(a)(3)(ii)(B)]

Establish risk designations and screening criteria for each position category that a workforce member is assigned to based on the risk posed by their level of access to facilities, information systems, and ePHI.

[NIST SP 800-53 PS-2]

Develop policies and procedures for screening individuals prior to authorizing their access to the information system.

[NIST SP 800-53 PS-3]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| \* The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the “Termination Checklist".  \* The Human Resources Department, users, and supervisors are required to notify the IS Help Desk to terminate a user’s access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):  \* The user has been using their access rights inappropriately;  \* A user’s password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);  \* An unauthorized individual is utilizing a user’s User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).  \* The Security Officer will terminate users’ access rights immediately upon notification.  \* The Security Officer audits and may terminate access of users that have not logged into organization’s information systems/applications for an extended period of time. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

[45 CFR §164.308(a)(3)(ii)(C)]

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

[NIST SP 800-53 PS-1]

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

[NIST SP 800-53 PS-4]

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

[NIST SP 800-53 PS-5]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| \* The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the “Termination Checklist".  \* The Human Resources Department, users, and supervisors are required to notify the IS Help Desk to terminate a user’s access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):  \* The user has been using their access rights inappropriately;  \* A user’s password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);  \* An unauthorized individual is utilizing a user’s User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).  \* The Security Officer will terminate users’ access rights immediately upon notification.  \* The Security Officer audits and may terminate access of users that have not logged into organization’s information systems/applications for an extended period of time. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.

[45 CFR §164.308(a)(3)(ii)(C)]

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

[NIST SP 800-53 PS-1]

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

# **A30 - §164.308(a)(4)(i) Standard** Do your practice’s policies and procedures describe the methods it uses to limit access to its ePHI?

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we cover these issues in our Systems Access policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

* Identity
* Role
* Biometric
* Proximity
* A combination of access methods

*Possible Threats and Vulnerabilities:*

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

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures for authorizing access to electronic protected health information that ate consistent with the applicable requirements of subpart E of this part.

[45 CFR §164.308(a)(4)(i)]

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

[NIST SP 800-53 AC-1]

Develop procedures to:

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

[NIST SP 800-53 AC-2]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we maintain a role based access policy in our Systems Access Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

[45 CFR §164.308(a)(4)(ii)(B)]

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

[NIST SP 800-53 AC-1]

Develop procedures to:

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

[NIST SP 800-53 AC-2]

* Employ the principles of least privilege/minimum necessary access for individuals so your practice only enables access to ePHI for users when it is necessary to accomplish the tasks assigned to them based on their roles.

[NIST SP 800-53 AC-6]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, we segregate access, roles, responsibilities to spread out the ability to provision accounts, permission access, and modify patient data. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures that, based upon the covered entity’s or business associate’s access authorization policies, establish document, review, and modify a user’s right of access to a workstation, transaction or program or process.

[45 CFR §164.308(a)(4)(ii)(C)]

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

[NIST SP 800-53 AC-1]

Develop procedures to:

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

[NIST SP 800-53 AC-2]

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| This is detailed in our Systems Access Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures that, based upon the entity’s access authorization policies, establish document, review, and modify a user’s right of access to a workstation, transaction or program or process.

[45 CFR §164.308(a)(4)(ii)(C)]

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

[NIST SP 800-53 AC-1]

Develop procedures to:

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We conduct a Security Awareness Training annually for all workforce members and upon hiring of any new members. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement a security awareness and training program for all members of its workforce (including management).

[45 CFR §164.308(a)(5)(i)]

Develop, document, and disseminate to workforce members a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance, and procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. The policy should also include procedures to facilitate its implementation and associated personnel security controls

[NIST SP 800-53 AT-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Security awareness training is updated on the same cadence as new recommendations come out of the risk management program to ensure alignment with up-to-date policies. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement a security awareness and training program for all members of its workforce (including management).

[45 CFR §164.308(a)(5)(i)]

Review and update the current security awareness and training policy and procedures based on environmental and operational changes affecting the security of ePHI.











[NIST SP 800-53 AT-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Role-based training is conducted for all new members. In addition, roles-based access controls are discussed as a part of new hire training and ongoing training to ensure proper security practices. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

A user is a person or entity with authorized access.

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice’s ePHI.
* Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.

Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals’ ability to diagnose and treat their patients.

*Examples of Safeguards:*

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

Implement a security awareness and training program for all members of its workforce (including management).

[45 CFR §164.308(a)(5)(i)]

Provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties

(when required by information system changes, and thereafter on an ongoing basis).

[NIST SP 800-53 AT-3]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Attendance is taken at all training sessions. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement a security awareness and training program for all members of its workforce (including management).

[45 CFR §164.308(a)(5)(i)]

Document and monitor individual information system security training activities including basic security awareness training and specific information system security training. Retain individual training records for workforce members and business associates.

[NIST SP 800-53 AT-4]

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

* Yes
* **No**

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We disseminate our security policies on a regular basis and conduct regular training. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
| We’ve set up a bimonthly security reminder schedule to ensure that reminders for security are sent to all those who have access to ePHI to follow proper security practices. |

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

* Low
* **Medium**
* High

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

* Low
* **Medium**
* High

**Overall Security Risk:**

* Low
* **Medium**
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Consider that security reminders can be:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Periodic security updates.

[45 CFR §164.308(a)(5)(ii)(A)]

Disseminate security alerts, advisories, and directives to workforce members.

[NIST SP 800-53 SI-5]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Our security awareness training contains slides specifically addressing software patches, security updates, and the importance of antivirus software updates. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider that:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Procedures for guarding against, detecting, and reporting malicious software.

[45 CFR §164.308(a)(5)(ii)(B)]

Establish procedures and oversight for installation of software by users; enforce software installation policies; and monitors policy compliance.

[NIST SP 800-53 CM-11]

# **A41 - §164.308(a)(5)(ii)(B) Addressable** Does your practice’s awareness and training content include information about how malware can get into your systems?

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We cover the specific methods by which malware can gain entry into our software systems. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Procedures for guarding against, detecting, and reporting malicious software.

[45 CFR §164.308(a)(5)(ii)(B)]

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

[NIST SP 800-53 AT-2]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We specifically detail the logging and monitoring requirements of the TowerView system |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Consider whether your practice makes its workforce members aware that:

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

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

*Possible Threats and Vulnerabilities:*

Your practice may not be able to safeguard its ePHI if its workforce members do not follow its policies and procedures regarding acceptable use of information systems and ePHI.

Some potential impacts include:

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

*Examples of Safeguards:*

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

Procedures for monitoring log-in attempts and reporting discrepancies.

[45 CFR §164.308(a)(5)(ii)(C)]

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

Employ automated mechanisms and tools to assist in the tracking of security incidents and in the collection and analysis of incident information, such as malware attacks.

[NIST SP 800-53 IR-5]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We detail what makes a good and bad password, and also our specific password requirements, in accordance with our security policies on password mgmt. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Procedures for creating, changing, and safeguarding passwords.

[45 CFR §164.308(a)(5)(ii)(D)]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We maintain an Audit Policy to monitor for unauthorized intrusion or disclosure and a Breach Policy to define our operating procedure in the event of a brief. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement policies and procedures to address security incidents.

[45 CFR §164.308(a)(6)(i)]

Develop, document, and disseminate to workforce members an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the incident response policy and associated incident response controls

[NIST SP 800-53 IR-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| ## Incident Management Policies  The TowerView Health incident response process follows the process recommended by SANS, an industry leader in security (www.sans.org). Process flows are a direct representation of the SANS process. Review Appendix 1 for a flowchart identifying each phase.  ### Identification Phase  1. Immediately upon observation TowerView Health members report suspected and known Precursors, Events, Indications, and Incidents in one of the following ways:  1. Direct report to management, the Security Officer, Privacy Officer, or other;  2. Email;  3. Phone call;  4. Online incident response form;  5. Secure Chat.  6. Anonymously through workforce members desired channels.  7. The individual receiving the report facilitates completion of an [Incident Identification form](./incident.form.pdf) and notifies the Security Officer (if not already done).  8. The Security Officer determines if the issue is a Precursor, Event, Indication, or Incident.  9. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.  1. Non-Technical Event (minor infringement): the Security Officer completes a SIR Form (see Appendix 2) and investigates the incident.  2. Technical Event: Assign the issue to an IT resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a small office or lack of expertise in the area.  10. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior management.  1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.  2. Once the investigation is completed, progress to Phase V, Follow-up.  3. If the issue is a technical security incident, commence to Phase II: Containment.  4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.  5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.  6. The lead member of the SIRT team facilitates initiation of a Security Incident Report (SIR) Form (See Appendix 2 for sample format) or an Incident Survey Form (See Appendix 4). The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.  11. The Security Officer, Privacy Officer, or TowerView Health representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.  12. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to TowerView Health and potentially external.  ### Containment Phase (Technical)  In this Phase, TowerView Health’s IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.  1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.  2. The SIRT secures the network perimeter.  3. The IT department performs the following:  1. Securely connect to the affected system over a trusted connection.  2. Retrieve any volatile data from the affected system.  3. Determine the relative integrity and the appropriateness of backing the system up.  4. If appropriate, back up the system.  5. Change the password(s) to the affected system(s).  6. Determine whether it is safe to continue operations with the affect system(s).  7. If it is safe, allow the system to continue to function;  1. Complete any documentation relative to the security incident on the SIR Form.  2. Move to Phase V, Follow-up.  8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.  9. The individual completing this phase provides written communication to the SIRT.  4. Continuously apprise Senior Management of progress.  5. Continue to notify affected Customers and Partners with relevant updates as needed  ### Eradication Phase (Technical)  The Eradication Phase represents the SIRT’s effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).  1. Determine symptoms and cause related to the affected system(s).  2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:  1. An increase in network perimeter defenses.  2. An increase in system monitoring defenses.  3. Remediation (“fixing”) any security issues within the affected system, such as removing unused services/general host hardening techniques.  3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.  1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.  4. Complete the Eradication Form (see Appendix 4).  5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).  6. Apprise Senior Management of the progress.  7. Continue to notify affected Customers and Partners with relevant updates as needed.  8. Move to Phase IV, Recovery.  ### Recovery Phase (Technical)  The Recovery Phase represents the SIRT’s effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.  1. The technical team determines if the affected system(s) have been changed in any way.  1. If they have, the technical team restores the system to its proper, intended functioning (“last known good”).  2. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).  3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.  4. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.  5. Update the documentation with the detail that was determined during this phase.  6. Apprise Senior Management of progress.  7. Continue to notify affected Customers and Partners with relevant updates as needed.  8. Move to Phase V, Follow-up.  ### Follow-up Phase (Technical and Non-Technical)  The Follow-up Phase represents the review of the security incident to look for “lessons learned” and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.  1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.  2. Create a “lessons learned” document and attach it to the completed SIR Form.  1. Evaluate the cost and impact of the security incident to TowerView Health using the documents provided by the SIRT and the technical security resource.  2. Determine what could be improved.  3. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.  4. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.  5. Close the security incident.  ### Periodic Evaluation  It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the TowerView Health’s expectation for them, relative to security responsibilities. The incident response plan is tested annually.  ## Security Incident Response Team (SIRT)  Individuals needed and responsible to respond to a security incident make up a Security Incident Response Team (SIRT). Members may include the following:  \* Security Officer  \* Privacy Officer  \* Senior Management  \* Lead Engineer |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

[45 CFR §164.308(a)(6)(ii)]

Develop, document, and disseminate to workforce members an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the incident response policy and associated incident response controls

[NIST SP 800-53 IR-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| The specific roles are detailed in our incident response policy and we conduct table top tests to verify plan success. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

[45 CFR §164.308(a)(6)(ii)]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| The incident response policy is reviewed in conjunction with the BC and DR plans to prioritize critical systems. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

If your practice’s incident response plan does not align with its emergency operations and contingency plan, it may not be able to safeguard its information systems, applications, and ePHI.

Some potential impacts include:

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

*Examples of Safeguards:*

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

[45 CFR §164.308(a)(6)(ii)]

Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

[NIST SP 800-53 IR-4]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| 14. ClamAV is run on all production hosts for anti-virus protection. Hosts are scanned daily for malicious binaries in critical system paths. The malware signature database is checked hourly and automatically updated if new signatures are available. ClamAV is a part of our Bash-based configuration management and this assures all hosts have anti-virus tools running on them. Workstations on Windows and Mac both run anti-virus hosts to protect against malware. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

[45 CFR §164.308(a)(6)(ii)]

Employs automated mechanisms and tools to assist in the tracking of security incidents and in the collection and analysis of incident information, such as malware attacks.











[NIST SP 800-53 IR-5]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We maintain a Business Continuity and Disaster Recovery policy to respond to natural or man-made disasters. Our production systems are designed to maintain uptime by switching over to backup servers in different regions as well. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Consider whether your practice’s contingency plan includes provisions:

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

[45 CFR §164.308(a)(7)(i)]

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

Develop, document, and disseminate to workforce members a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

[NIST SP 800-53 CP-1]

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

Implement a contingency plan that identifies roles and responsibilities for accessing ePHI and also identifies the critical information systems that are needed during an emergency.

[NIST SP 800-53 CP-2]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| The contingency plan is reviewed after any major emergency, security incident, and during risk assessment review. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

[45 CFR §164.308(a)(7)(i)]

Review and update the current contingency planning policy and contingency planning procedures regularly or as needed.

[NIST SP 800-53 CP-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| We store weekly backup copies of ePHI that can be recovered that are distributed across other regions. Our backup procedures are detailed in the Data Management Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals’ ability to diagnose and treat their patients.

*Examples of Safeguards:*

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

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

[45 CFR §164.308(a)(7)(ii)(A)]

Develop, document, and disseminate to workforce members a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls

[NIST SP 800-53 CP-1]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| # Disaster Recovery Policy  The TowerView Health Contingency Plan establishes procedures to recover TowerView Health following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the TowerView Health Security Officer and Privacy Officer.  The following objectives have been established for this plan:  1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:  \* \*Notification/Activation phase\* to detect and assess damage and to activate the plan;  \* \*Recovery phase\* to restore temporary IT operations and recover damage done to the original system;  \* \*Reconstitution phase\* to restore IT system processing capabilities to normal operations.  2. Identify the activities, resources, and procedures needed to carry out TowerView Health processing requirements during prolonged interruptions to normal operations.  3. Identify and define the impact of interruptions to TowerView Health systems.  4. Assign responsibilities to designated personnel and provide guidance for recovering TowerView Health during prolonged periods of interruption to normal operations.  5. Ensure coordination with other TowerView Health staff who will participate in the contingency planning strategies.  6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.  This TowerView Health Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.  This TowerView Health Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.    The TowerView Health Contingency Plan also complies with the following federal and departmental policies:  \* The Computer Security Act of 1987;  \* OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000;  \* Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;  \* Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, OCOOber 1998;  \* PDD 63, Critical Infrastructure Protection, May 1998;  \* Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;  \* Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” OCOOber 30, 2000  Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, internal malicious activities.  TowerView Health defined two categories of systems from a disaster recovery perspective.  1. \*Critical Systems\*. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.  2. \*Non-critical Systems\*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.  ## Applicable Standards from the HITRUST Common Security Framework  \* 12.c - Developing and Implementing Continuity Plans Including Information Security  ## Applicable Standards from the HIPAA Security Rule  \* 164.308(a)(7)(i) - Contingency Plan  ## Line of Succession  The following order of succession to ensure that decision-making authority for the TowerView Health Contingency Plan is uninterrupted. The Chief Operating Officer (COO) and Security Officer, Hareesh Ganesan, are responsible for ensuring the safety of personnel and the execution of procedures documented within this TowerView Health Contingency Plan. If the COO and Lead engineer are unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO shall function as that authority. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.  \* Hareesh Ganesan, COO: 301-943-6475, hareesh@towerviewhealth.com  \* Osuvaldo Ramos, Lead Engineer: 817-914-8218, osuvaldo@towerviewhealth.com  \* Rahul Jain, CEO: 715-771-9831, rahul@towerviewhealth.com  ## Responsibilities  The following teams have been developed and trained to respond to a contingency event affecting the IT system.  1. The \*\*Engineering Team\*\* is responsible for recovery of the TowerView Health hosted environment, network devices, and all servers. Members of the team include personnel who are also responsible for the daily operations and maintenance of TowerView Health. The team leader is the COO and directs the Dev Ops Team.  2. The \*\*Engineering Team\*\* is responsible for assuring all application servers, web services, and platform add-ons are working. It is also responsible for testing redeployments and assessing damage to the environment. The team leader is the COO and directs the Web Services Team.  ## Testing and Maintenance  The COO and Lead Engineer shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan’s execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.  ### Tabletop Testing  Tabletop Testing is conducted in accordance with the the CMS Risk Management Handbook, Volume 2 (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH\_VII\_4-5\_Contingency\_Plan\_Exercise.pdf). The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:  \* Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.  ### Technical Testing  The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:  \* Process from backup system at the alternate site;  \* Restore system using backups; and  \* Switch compute and storage resources to alternate processing site.  ## 1. Notification and Activation Phase  This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to TowerView Health. Based on the assessment of the Event, sometimes according to the TowerView Health Incident Response Policy, the Contingency Plan may be activated by either the COO or Lead Engineer.  The notification sequence is listed below:  \* The first responder is to notify the COO. All known information must be relayed to the COO.  \* The Lead Engineer is to contact the Web Services Team and inform them of the event. The COO is to to begin assessment procedures.  \* The COO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the COO is to follow the steps below.  \* Damage Assessment Procedures:  \* The COO and Lead Engineer are to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.  \* Alternate Assessment Procedures:  \* Upon notification from the COO, the Lead Engineer is to follow the procedures for damage assessment with combined Dev Ops and Web Services Teams.  \* The TowerView Health Contingency Plan is to be activated if one or more of the following criteria are met:  \* TowerView Health will be unavailable for more than 48 hours.  \* Hosting facility is damaged and will be unavailable for more than 24 hours.  \* Other criteria, as appropriate and as defined by TowerView Health.  \* If the plan is to be activated, the COO is to notify and inform team members of the details of the event and if relocation is required.  \* Upon notification from the COO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.  \* The COO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.  \* The COO is to notify remaining personnel and executive leadership on the general status of the incident.  \* Notification can be message, email, or phone.  ## 2. Recovery Phase  This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.  The following procedures are for recovering the TowerView Health infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.  Recovery Goal: The goal is to rebuild TowerView Health infrastructure to a production state.  The tasks outlines below are not sequential and some can be run in parallel.  1. Contact Partners and Customers affected  2. Assess damage to the environment  3. Begin replication of new environment using automated and tested scripts, currently Bash.  4. Test new environment using pre-written tests  5. Test logging, security, and alerting functionality  6. Assure systems are appropriately patched and up to date.  7. Deploy environment to production  8. Update DNS to new environment.  ## 3. Reconstitution Phase  This section discusses activities necessary for restoring TowerView Health operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, TowerView Health operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.  1. Original or New Site Restoration  \* Begin replication of new environment using automated and tested scripts, currently Bash.  \* Test new environment using pre-written tests.  \* Test logging, security, and alerting functionality.  \* Deploy environment to production  \* Assure systems are appropriately patched and up to date.  \* Update DNS to new environment.  2. Plan Deactivation  If the TowerView Health environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the TowerView Health Media Disposal Policy. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Establish (and implement as needed) procedures to restore any loss of data.

[45 CFR §164.308(a)(7)(ii)(B)]

Develop, document, and disseminate to workforce members a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls;

[NIST SP 800-53 CP-1]

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

Conduct backups of user-level, system- level, and security-related documentation contained in the information system.











[NIST SP 800-53 CP-9]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| ### Tabletop Testing  Tabletop Testing is conducted in accordance with the the CMS Risk Management Handbook, Volume 2 (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH\_VII\_4-5\_Contingency\_Plan\_Exercise.pdf). The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:  \* Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Implement procedures for periodic testing and revisions of contingency plans.

[45 CFR §164.308(a)(7)(ii)(D)]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| TowerView Health defined two categories of systems from a disaster recovery perspective.  1. \*Critical Systems\*. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.  2. \*Non-critical Systems\*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Assess the relative criticality of specific applications and data in support of other contingency plan components.

[45 CFR §164.308(a)(7)(ii)(E)]

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

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

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

Categorize information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

[NIST SP 800-53 RA-2]

Document the security categorization results (including supporting rationale) in the security plan for the information system.

[NIST SP 800-53 RA-2]

Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official’s designated representative.

[NIST SP 800-53 RA-2]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| 2. Risk analysis and risk management are recognized as important components of TowerView Health’s corporate compliance program and information security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).  1. Risk assessments are done throughout product life cycles:  2. Before the integration of new system technologies and before changes are made to TowerView Health physical safeguards; and  \* These changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and management of the TowerView Health Platform.  3. While making changes to TowerView Health physical equipment and facilities that introduce new, untested configurations.  4. TowerView Health performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(a)(8)]

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

[NIST SP 800-53 RA-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(a)(8)]

Monitor information systems to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections. Deploy monitoring devices to identify unauthorized use of information systems.

[NIST SP 800-53 SI-4]

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, our Security Officer is responsible and accountable for assessing risk and engaging in ongoing evaluation, monitoring, and reporting. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(a)(8)]

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

[NIST SP 800-53 RA-1]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Yes, these are the duties of the company’s Privacy Officer. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

* Service providers are unaware of the types of sensitive information that they will possess or control when performing the services on your behalf and fail to take reasonable care to protect the privacy and security of ePHI.
* Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice’s ePHI.
* Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
* Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals’ ability to diagnose and treat their patients.

*Examples of Safeguards:*

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

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

[45 CFR §164.308(b)(1)]

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(b)(1)]

Develop processes to establish and maintain a list of authorized maintenance organizations or personnel which identifies their level of access to facilities, information systems, and ePHI.

[NIST SP 800-53 MA-5]

Develop processes to establish and monitor the security roles and responsibilities of 3rd party providers who access the practice facilities, information systems, and ePHI.

[NIST SP 800-53 PS-7]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

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

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(b)(1)]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| # 3rd Party Policy  TowerView Health makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of TowerView Health or TowerView Health Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.  ## Applicable Standards from the HITRUST Common Security Framework  \* 05.i - Identification of Risks Related to External Parties  \* 05.k - Addressing Security in Third Party Agreements  \* 09.e - Service Delivery  \* 09.f - Monitoring and Review of Third Party Services  \* 09.g - Managing Changes to Third Party Services  \* 10.1 - Outsourced Software Development  ## Applicable Standards from the HIPAA Security Rule  \* 164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements  ## Policies to Assure 3rd Parties Support TowerView Health Compliance  1. The following steps are required before 3rd parties are granted access to any TowerView Health systems:  \* Due diligence with the 3rd party;  \* Controls implemented to maintain compliance;  \* Written agreements, with appropriate security requirements, are executed.  2. All connections and data in transit between the TowerView Health Platform and 3rd parties are encrypted end to end. Data in transit is encrypted using SSL protocols and data at rest is encrypted using AES-256 bit encryption.  3. Access granted to external parties is limited to the minimum necessary and granted only for the duration required.  4. A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization’s security policies. Additionally, responsibility is assigned in these agreements.  5. TowerView Health has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of services management.  \* TowerView Health utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.  7. Third parties are unable to make changes to any TowerView Health infrastructure without explicit permission from TowerView Health. Additionally, no TowerView Health Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.  8. Whenever outsourced development is utilized by TowerView Health, all changes to production systems will be approved and implemented by TowerView Health workforce members only. All outsourced development requires a formal contract with TowerView Health.  9. TowerView Health maintains and annually reviews a list all current Partners and Subcontractors.  10. TowerView Health assesses security requirements and compliance considerations with all Partners and Subcontracts. This includes annual assessment of SOC2 Reports for all TowerView Health infrastructure partners.  \* TowerView Health leverages recurring calendar invites to assure reviews of SLAs with all 3rd parties are performed annually. These are performed by the TowerView Health Security Officer and Privacy Officer. Google Forms are used to track such reviews.  11. Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.  13. Any changes to Partner and Subcontractor services and systems are reviewed before implementation.  14. For all partners, TowerView Health reviews activity annually to assure partners are in line with SLAs in contracts with TowerView Health. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

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

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

*Examples of Safeguards:*

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| 4. A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization’s security policies. Additionally, responsibility is assigned in these agreements. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Satisfactory assurances include but are not limited to:

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.308(b)(3)]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* Low
* Medium
* High

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

* Low
* Medium
* High

**Overall Security Risk:**

* Low
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

Satisfactory assurances include but are not limited to:

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.314(a)(1)(i)]

Satisfactory assurances include but are not limited to:

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

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Please review the TowerView BAA. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

Satisfactory assurances include but are not limited to:

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.314(a)(2)(i)]

Satisfactory assurances include but are not limited to:

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

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.314(a)(2)(iii)]

Satisfactory assurances include but are not limited to:

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

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

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| 1. It is the policy of TowerView Health to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) (and other confidential and proprietary electronic information) it stores, transmits, and/or processes for its Customers and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the TowerView Health's information security program.  2. Risk analysis and risk management are recognized as important components of TowerView Health’s corporate compliance program and information security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).  1. Risk assessments are done throughout product life cycles:  2. Before the integration of new system technologies and before changes are made to TowerView Health physical safeguards; and  \* These changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and management of the TowerView Health Platform.  3. While making changes to TowerView Health physical equipment and facilities that introduce new, untested configurations.  4. TowerView Health performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.  3. TowerView Health implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:  1. Ensure the confidentiality, integrity, and availability of all ePHI TowerView Health receives, maintains, processes, and/or transmits for its Customers;  2. Protect against any reasonably anticipated threats or hazards to the security or integrity of Customer ePHI;  3. Protect against any reasonably anticipated uses or disclosures of Customer ePHI that are not permitted or required; and  4. Ensure compliance by all workforce members.  4. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management and TowerView Health’s Security Officer.  5. All TowerView Health workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation, as outlined in the TowerView Health Roles Policy.  6. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of TowerView Health’s Security Officer (or other designated employee), and the identified Risk Management Team.  7. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.316(a)]

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

[NIST SP 800-53 RA-1]

Document, review, and disseminate risk assessment results to members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified as a result of a risk assessment.

[NIST SP 800-53 RA-3]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Our policies and procedures are maintained in a publicly available internal repository. This repository is revision controlled to allow for tracking and review of changes over time. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Maintain the policies and procedures implemented to comply with this subpart (i.e. HIPAA Security Rule) in written (which may be electronic) form.

[45 CFR §164.316(b)(1)(i)]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| All documentation is stored together and revision controlled in either internal Git repository or a cloud drive that is regularly backed up. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

If an action, activity or assessment is required by this subpart (i.e. HIPAA Security Rule) to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

[45 CFR §164.316(b)(1)(ii)]

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

[[NIST SP 800-53 SI-12]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

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

[45 CFR §164.316(b)(2)(i)]

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

[NIST SP 800-53 SI-12]

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

[NIST SP 800-53 AU-7]

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
| Documents are shared and permissioned to all pertinent workforce members. |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

[45 CFR §164.316(b)(2)(ii)]

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

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

* **Yes**
* No

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

* Cost
* Practice Size
* Complexity
* Alternate Solution

Please detail your current activities:

|  |
| --- |
|  |

Please include any additional notes:

|  |
| --- |
|  |

Please detail your remediation plan:

|  |
| --- |
|  |

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

* **Low**
* Medium
* High

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

* **Low**
* Medium
* High

**Overall Security Risk:**

* **Low**
* Medium
* High

**Related Information:**

*Things to Consider to Help Answer the Question:*

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

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

*Possible Threats and Vulnerabilities:*

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

Some potential impacts include:

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

*Examples of Safeguards:*

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

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[45 CFR §164.316(b)(2)(iii)]

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

[NIST SP 800-53 PL-1]

Review and update the current security policy and security planning procedures.

[NIST SP 800-53 PL-2]

1. http://www.hhs.gov/hipaa/index.html [↑](#footnote-ref-1)
2. https://www.healthit.gov/ [↑](#footnote-ref-2)
3. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\_30\_r1.pdf [↑](#footnote-ref-3)