

Version: 0.1

**2024 NIST CSF 2.0 Annual Risk Assessment**  
  
**Review Type:** 2024 NIST CSF 2.0 Annual Risk Assessment

**Completion:** MM/DD/YYY

**Policy Area:** Information Security Risk Management Policy and Procedure

**Applicability:** Organization Company-wide

BLANK PAGE



|  |  |
| --- | --- |
|  | Decorative |
|  | SUMMARY |
|  | The Compliance Team is pleased to present this overview of the annual ORGANIZATION HIPAA Risk Assessment. The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of sensitive health information, and our commitment to compliance necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).  This report provides insight into the objectives and methodology of our HIPAA risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA regulations. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI.  We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the privacy and security of health information. |

Table of Contents

[ 1](#_Toc150852620)

[SUMMARY 1](#_Toc150852621)

[Introduction 3](#_Toc150852622)

[Objectives 3](#_Toc150852623)

[Regulatory Framework 4](#_Toc150852624)

[Risk Assessment Methodology 4](#_Toc150852625)

[Risk Identification 6](#_Toc150852626)

[Goals for 2023/2024 7](#_Toc150852627)

[SOC 2 Type II Updated Audit (2023/24) 7](#_Toc150852628)

[HITRUST i1 Audit (2024) 7](#_Toc150852629)

[Roadmap for the Future 8](#_Toc150852630)

[WHAT’S NEXT 9](#_Toc150852631)

[Results Year over Year 2022 - 2023 11](#_Toc150852632)

[Summary for each HIPAA Sub-Section 12](#_Toc150852633)

[APPENDIX A: HIPAA RISK ASSESSMENT WORK PAPERS 13](#_Toc150852634)

|  |  |
| --- | --- |
| Maturity continues to grow and move in the right direction  A graph of different colored rectangular shapes  Description automatically generated | Decorative |
|  | Introduction |
|  | The Compliance Team is pleased to present this overview of the annual ORGANIZATION HIPAA Risk Assessment, based on NIST 800-66r1. The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of sensitive health information, and our commitment to compliance necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).  This report provides insight into the objectives and methodology of our HIPAA risk assessment. We aim to identify and analyze risks, ensuring our security measures align with HIPAA regulations. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI.  We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the privacy and security of health information. Objectives The primary objectives of the Annual ORGANIZATION HIPAA risk assessment are to:   * Discover and document potential risks to the security of PHI. * Assess the potential impact and likelihood of each identified risk on the confidentiality, integrity, and availability of PHI. * Ensure that the organization's policies and procedures align with HIPAA requirements and that employees adhere to established security measures. * Identify gaps between current security measures and the requirements outlined in the HIPAA Security Rule. * Develop strategies and action plans to mitigate and manage identified risks effectively. * Maintain thorough documentation of the risk assessment process, findings, and recommendations. * Establish a framework for continuous monitoring, auditing, and updating security measures to adapt to evolving threats and changes in the organization's environment.    Regulatory Framework The HIPAA Security and Privacy Rules are integral to the Health Insurance Portability and Accountability Act, designed to safeguard the confidentiality, integrity, and availability of protected health information (PHI). The Security Rule establishes standards for the security of electronic PHI, requiring healthcare organizations to implement measures such as access controls, encryption, and audit trails to protect sensitive data. On the other hand, the Privacy Rule focuses on defining and limiting how healthcare providers and organizations use and disclose individuals' health information. Together, these rules aim to ensure the privacy and security of PHI, enhance patients' control over their health information, and maintain the trust and integrity of the healthcare system.  **HIPAA regulations extend beyond healthcare providers to encompass business associates**  HIPAA regulations extend beyond healthcare providers to encompass business associates engaged in activities involving electronic protected health information (ePHI) on behalf of covered entities. ORGANIZATION (a business associate) must adhere to the HIPAA Privacy Rule, governing PHI use and disclosure, and the Security Rule, mandating safeguards for ePHI. The Breach Notification Rule requires ORGANIZATION to report breaches of unsecured ePHI, and the Enforcement Rule outlines penalties for non-compliance. The HIPAA Omnibus Rule expanded business associates' responsibilities, making them directly liable for specific Privacy and Security Rule provisions. The pivotal Business Associate Agreement (BAA) establishes contractual obligations between business associates and covered entities. Compliance with these regulations is essential, as failure to do so can result in legal repercussions and loss of patient data, underscoring the critical role of business associates in maintaining the privacy and security of healthcare information. Risk Assessment Methodology In conducting the Annual 2023 HIPAA risk assessment, information was gathered from several sources to understand and evaluate ORGANIZATION’s security landscape against HIPAA. The process began with identifying all information systems that process, transmit, or store ePHI, encompassing data repositories, systems, networks, hardware, software, and personnel. The assessment identified potential threats, including natural disasters, human errors, malicious attacks, and technical failures. Simultaneously, vulnerabilities in systems and processes are assessed, often involving thorough reviews of configurations, penetration testing, and an analysis of existing security controls. The effectiveness of current security measures, such as access controls, encryption, and incident response procedures, is also evaluated.  The assessment followed the guidelines and standards outlined in the HIPAA Security Rule and NIST Special Publication 800-66 for guidance in safeguarding PHI. Additionally, regulatory compliance requirements pertinent to ORGANIZATION’s operations were considered, ensuring alignment with HIPAA. The process incorporated interviews with key stakeholders, documentation reviews, and analyses of historical data, including past security assessments. The culmination of this information allowed for a holistic understanding of ORGANIZATION’s risk landscape, facilitating informed decision-making for risk prioritization and mitigation strategies.  Within the landscape of healthcare information security, the National Institute of Standards and Technology (NIST) has crafted a guide known as NIST 800-66. This guide, titled "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," serves as a comprehensive roadmap for ORGANIZATION to fortify their information technology security practices.  **NIST 800-66 provides the overarching scope and purpose of the HIPAA Security Rule**  At its core, NIST 800-66 provides the overarching scope and purpose of the HIPAA Security Rule, emphasizing the safeguard electronic protected health information (ePHI). Acting as a foundational resource, the guide illuminates the security requirements mandated by HIPAA, paving the way for organizations to align their practices accordingly.  Emphasizing a holistic security management process, NIST 800-66 delves into key components such as risk assessment, policy development, workforce training, and ongoing monitoring. The guide sheds light on technical safeguards, including access controls, audit controls, and integrity controls, offering insights into their implementation and maintenance to secure electronic health information.  Additionally, NIST 800-66 underscores the importance of incident response and contingency planning. It provides guidance on developing effective strategies to respond to security incidents and ensuring business continuity in the face of disruptions.  The guide also places significance on security awareness and training programs, recognizing their pivotal role in cultivating a culture of security within healthcare organizations. By offering guidance on educating staff to recognize and address security risks, NIST 800-66 aims to fortify the human element in information security.  Finally, NIST 800-66 advocates for ongoing compliance monitoring and evaluation of security controls. It encourages organizations to regularly assess and update their security measures, aligning them with evolving threats and technological advancements.  In essence, NIST 800-66 emerges as a vital resource, guiding healthcare organizations through the intricate landscape of HIPAA compliance. Its practical insights empower entities to fortify their information technology security, ensuring the confidentiality, integrity, and availability of electronic protected health information.  Risk Identification  * ORGANIZATION does not have a documented Business Continuity plan as per §164.308(a)(7)(i) which states, "Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information." In addition to prevention, the goal is to enable ongoing operations before and during the execution of disaster recovery. Business continuity is the intended outcome of properly executing business continuity planning and disaster recovery. With a Business Continuity Plan, ORGANIZATION will know how to keep the business going during an adverse incident.   **Audit & Log Monitoring and Business Continuity Planning continues to be a challenge.**  **Access Control reviews, to include those that have changed job roles, for systems that process, transmit or store ePHI is lacking.**   * Logs are being captured for all critical ePHI systems, and there is a requirement to formally monitor the logs and address all alerts on a regular cadence, but monitoring is not being done. A lack of monitoring could lead to anomalous activity that could go unnoticed for a lengthy period of time. * There is no comprehensive review of access control for systems that process, transmit, or store ePHI on a specified frequency. Lack of access control reviews could lead to a potential past employee or a current transfer employee having more access than they need or having access after they leave ORGANIZATION. * There is no logon banner to ORGANIZATION endpoints stating that this device is the property of ORGANIZATION and there should be no expectation of privacy on ORGANIZATION-owned devices. ORGANIZATION does not have a login banner stating that ORGANIZATION owns the ORGANIZATION device and that there is no expectation of privacy on ORGANIZATION-owned devices. * There is no documented process for when a workforce member changes roles. There needs to be a documented process to ensure users are transferred to a new role in ORGANIZATION. A lack of transfer procedure roles will lead to access creep. * There is no formal documented process to review system tools, misuse, abuse, and fraudulent activity. Lack of reviewing tools (e.g., CoPilot to GitHub or MacBook notes to stored passwords or ePHI) could leave ORGANIZATION open to unauthorized applications, applications with vulnerabilities, or applications where Terms and Services state that open-source software cannot be used for corporate purposes without a license.      * Job descriptions help identify particular skills or abilities necessary for a given position. There is a lack of Job Descriptions that specifically state what data a user can access, for example, ePHI. This will help IT determine what systems they are allowed to access. |

|  |  |  |
| --- | --- | --- |
|  |  | Decorative |
| ORGANIZATION Maturity   * ORGANIZATION is 90% Compliance with HIPAA Security & Privacy Regulations   ADDED  PRIORITIES   * SOC 2 Type II * HITRUST i1 * 21 CFR 11 * On the Horizon, GDPR, FedRamp   Control Owners   * Identify / Re-identify Controls Owners * Identify control that apply to each control owner. * Owners gather evidence to illustrate compliance with industry frameworks. |  | Goals for 2023/2024 |
| SOC 2 Type II Updated Audit (2023/24) The following are the next steps for the soc 2 audit.   1. **Pre-Audit Review:** Conduct a thorough pre-audit review to identify any potential gaps or areas for improvement in our SOC 2 compliance. 2. **Refinement of Controls:** Fine-tune and optimize our security controls based on any feedback received during the pre-audit review. 3. **Communication Plan:** Develop a clear communication plan to keep all stakeholders informed throughout the audit process, ensuring transparency and alignment.  HITRUST i1 Audit (2024) ORGANIZATION is embarking on the implementation of the HITRUST Common Security Framework (CSF), which is a strategic endeavor that demands careful consideration and methodical execution. The initial steps involve defining the scope and objectives of the HITRUST initiative, delineating the systems, processes, and data within its purview. Subsequently, organizations must familiarize themselves with the comprehensive HITRUST CSF framework, absorbing its multifaceted controls and requirements, which draw from various industry standards.  A pivotal aspect of the implementation process is conducting a thorough risk self-assessment to identify potential threats to sensitive data, guiding subsequent actions and priorities. Furthermore, the implementation journey includes the deployment of a suite of security controls, covering technical, administrative, and physical dimensions to fortify information security.  As ORGANIZATION progresses, it must establish effective third-party management practices, train its workforce on security protocols, and develop robust incident response and business continuity plans. Continuous monitoring mechanisms are instituted to detect and respond to evolving security threats. Preparation for the formal HITRUST assessment involves engaging with qualified assessors and meticulous documentation. Through this assessment and subsequent actions to address identified gaps, the organization works towards achieving and maintaining HITRUST certification, a testament to its commitment to ongoing compliance and the secure handling of healthcare information. Regular assessments, updates, and collaboration with HITRUST-authorized assessors are integral elements, ensuring the organization's resilience in the dynamic landscape of information security and regulatory requirements. Roadmap for the Future ORGANIZATION has several audits on the horizon for SOC 2 and HITRUST i1. The Compliance team, working with the Compliance, Security, and Privacy Committee to set the future roadmap… |

|  |  |
| --- | --- |
| Continue navigating SOC 2 & HITRUST i1 | Decorative |
|  | WHAT’S NEXT |
|  | As we navigate the path towards HITRUST CSF i1 validated assessment and SOC update, it is crucial to acknowledge and address the findings uncovered during our recent evaluations. These findings serve as valuable insights that guide our journey towards enhancing the security posture of our organization.  The next phase involves a strategic and collaborative approach to remediate the identified issues. Our primary objective is to bolster our security controls, aligning them with the rigorous standards set forth by HITRUST and SOC. This entails a comprehensive review and response to each finding, prioritizing actions based on their impact and severity.  **Key Steps in the Remediation Process:**   1. **Detailed Analysis:** Conduct an in-depth analysis of each finding to understand its root cause, potential impact, and the optimal path for resolution. Engage relevant stakeholders to gain diverse perspectives on the identified issues. 2. **Prioritization:** Prioritize the findings based on their criticality and potential risk to our organization. 3. **Action Plans:** Develop detailed action plans for each finding, outlining specific steps, responsible parties, and timelines for resolution. These plans should be comprehensive, addressing not only the immediate concerns but also establishing preventive measures for the future. 4. **Collaborative Efforts:** Remediation is a collective effort. Engage cross-functional teams, involving IT, security, compliance, and relevant business units to collaboratively work towards resolving the findings. Foster clear communication channels to ensure everyone is aligned on the remediation goals. 5. **Continuous Monitoring:** Implement continuous monitoring mechanisms to track the progress of remediation efforts. Regularly review and update the status of each finding to maintain transparency and accountability throughout the process. 6. **Documentation and Evidence:** Thoroughly document the remediation process, including evidence of corrective actions taken. This documentation is not only essential for audit purposes but also serves as a valuable resource for continuous improvement. 7. **Training and Awareness:** Consider the findings as opportunities for learning and improvement. Provide additional training and awareness programs to relevant staff members to prevent the recurrence of similar issues.   **Communication Plan:**  **ORGANIZATION continues to mature its Privacy and Information Security Program**  Maintaining open and transparent communication is paramount. Establish a communication plan to keep all stakeholders informed about the progress of remediation efforts. Regular updates, status reports, and any adjustments to the remediation plan should be communicated promptly to ensure everyone is on the same page.  **Continuous Improvement:**  As we address these findings, let's view this process as an integral part of our commitment to continuous improvement. Embrace the opportunity to strengthen our security posture, aligning it not only with HITRUST and SOC requirements but also with the ever-evolving landscape of cybersecurity threats.  Through a concerted and diligent effort, we aim to not only rectify the identified issues but to emerge from this process with a more resilient and secure foundation. Our collective dedication to these remediation efforts will undoubtedly contribute to our long-term success in maintaining a robust security framework.  A graph of different colored rectangular shapes  Description automatically generated |

|  |
| --- |
| Decorative |
| Results Year over Year 2022 - 2023 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 2020 Controls Measured | 2022 Compliance Score | 2023 Controls Measured | 2023 Compliance Score | | 164.308 Administrative Controls | 63 | 87% | 185 | 85% | | 164.310 Physical Safeguards | 20 | N/A | 95 | N/A | | 164.312 Technical Safeguards | 25 | 100% | 80 | 82% | | 164.314 Organizational Requirements | 4 | 100% | 23 | 100% | | 164.316 Policy, Procedure, Documentation Requirements | 8 | 100% | 16 | 100% | | **Total Controls** | **120** | **97%** | **399** | **92%** |   In 2022, ORGANIZATION conducted a HIPAA risk assessment looking at 120 controls to create a baseline for the minimum level of security and privacy to identify risks. Physical Safeguards do not apply to ORGANIZATION as ORGANIZATION is 100% remote workforce. Physical safeguards are handled by ORGANIZATION third-party computing services. ORGANIZATION did not use a framework for the 2022 and past assessments.  In 2023, ORGANIZATION used NIST 800-66r1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.” NIST 800-66r1 summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. Summary for each HIPAA Sub-Section **164.308 Administrative Controls:**  The organization demonstrates a commendable level of compliance with administrative controls, scoring at 85%. This reflects a robust implementation of measures governing security management processes, workforce training, and information access management. However, there may be areas for improvement to achieve full compliance. See Risk Register for more information on observations.  **164.310 Physical Safeguards:**  Given the organization's 100% remote nature, the HIPAA standard 164.310 for physical safeguards does not apply. Remote organizations are exempt from certain physical security requirements, acknowledging the unique operational context.  **164.312 Technical Safeguards:**  The organization is 82% compliant with technical safeguards, indicating a substantial adherence to security measures related to access controls, audit controls, integrity controls, and transmission security. While a strong foundation is in place, there may be opportunities to enhance compliance in specific technical areas.  **164.314 Organizational Requirements:**  The organization demonstrates exemplary compliance with organizational requirements, achieving a perfect score of 100%. This reflects a robust commitment to implementing policies and procedures to protect electronic protected health information (ePHI) and manage potential risks effectively.  **164.316 Policy, Procedure, Documentation, and Requirements:**  The organization is fully compliant with policies, procedures, documentation, and requirements, achieving a 100% score. This indicates a comprehensive and well-documented approach to maintaining and implementing policies that safeguard ePHI in accordance with HIPAA regulations. |
|  |
|  |
|  |

## APPENDIX A: HIPAA RISK ASSESSMENT WORK PAPERS

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **HIPAA Reg** | **HIPAA Topic** | **HIPAA Reg Description** | **Question Text** | SRA Answer | **Risk Identified** | **Risk Level** | **Assessors Explanation** |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization developed, disseminated, reviewed/updated, and trained on your Risk Assessment policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has an ISMP with applicable documented policies, procedures and standards. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Does your organization's risk assessment policy address: purpose, scope, roles and responsibilities management commitment, coordination among organizational entities, training and compliance? | HIPAA Reg Met | No | N/A | ORGANIZATION has a comprehensive risk management and risk assessment program that has been communicated to applicable individuals |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization disseminated your Risk Assessment policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a comprehensive risk management and risk assessment program that has been communicated to applicable individuals |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization disseminated its Risk Assessment procedures to the work staff/offices with the associated roles and responsibilities? | HIPAA Reg Met | No | N/A | ORGANIZATION works with the internal Compliance Committee, who are the risk managers to determine risks. This is a bi-monthly meetings where risk education is trained upon. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization defined the frequency of your Risk Assessment policy and procedures reviews and updates? | HIPAA Reg Met | No | N/A | The ORGANIZATION Information Security Program Policy states that we need to update our policies at least annually for when a significant change happens. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization reviewed and updated your Risk Assessment policy and procedures in accordance with your defined frequency? | HIPAA Reg Met | No | N/A | The ORGANIZATION Information Security Program Policy states that we need to update our policies at least annually for when a significant change happens. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization identified the **types** of information and **uses** of that information and the **sensitivity** of each **type** of information been evaluated (also link to FIPS 199 and SP 800-60 for more on categorization of sensitivity levels)? | HIPAA Reg Met | No | N/A | ORGANIZATION has an approved Data Classification Policy and Standard however ORGANIZATION does not have a program to clearly document and illustrate when data is PHI. There is no formal labeling of records. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization identified all information systems that house ePHI? | HIPAA Reg Met | No | N/A | All systems containing PHI have been identified. This is evidenced by the SOC 2 Type 2 of 2023 scope. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Does your organization inventory include all hardware and software that are used to collect, store, process, or transmit ePHI, including excel spreadsheets, word tables, and other like data storage? | HIPAA Reg Met | No | N/A | ORGANIZATION has an inventory for all hardware and software apps regardless of ePHI or not. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Are all the hardware and software for which your organization is responsible periodically inventoried, including excel spreadsheets, word tables, and other like data storage? | HIPAA Reg Met | No | N/A | ORGANIZATION has an inventory for all hardware and software apps regardless of ePHI or not. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Has your organization identified all hardware and software that maintains or transmits ePHI, including excel spreadsheets, word tables, and other similar data storage and included it in your inventory? | HIPAA Reg Met | No | N/A | ORGANIZATION needs to identify all hardware and software that maintains and transmits ePHI. This includes workstations. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Does your organization's inventory include removable media, remote access devices, and mobile devices? | HIPAA Reg Met | No | N/A | ORGANIZATION has an inventory for all hardware and software apps regardless of ePHI or not. |
| 164.308(a)(1)(i) | Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations | The security management process includes all the written policies and procedures used to stop, find, and fix any security mistakes, that can be either events or something you omitted. | Is the current information system configuration documented, including connections to other systems, both inside and outside your firewall? | HIPAA Reg Met | No | N/A | ORGANIZATION has current information system configuration documented, including connections to other systems, both inside and outside your firewall. |
| 164.308(a)(1)(ii) | Implementation specifications | Implementation specifications for security management process | Has your organization reviewed all processes involving ePHI, including creating, receiving, maintaining, and transmitting it? | HIPAA Reg Met | No | N/A | All critical processes have been reviewed during the SOC 2 Type 2 of 2023 |
| 164.308(a)(1)(ii) | Implementation specifications | Implementation specifications for security management process | Has your organization reviewed the risk analysis and other implementation specifications for the security management process? | HIPAA Reg Met | No | N/A | ORGANIZATION has a documented risk assessment procedure and process. In addition, ORGANIZATION has a comprehensive Risk Register that is used to capture specifications are not in compliance and track them to closure |
| 164.308(a)(1)(ii) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI. A risk assessment methodology, based on NIST SP 800-30, is included in Appendix E of this document. | Implementation specifications for security management process | Does your organization have any prior risk assessments, audit comments, security requirements, and/or security test results? | HIPAA Reg Met | No | N/A | ORGANIZATION has conducted HIPAA Risk Assessments, SOC 2 Type 2 Assessments and HITRUST i1, which is an annual audit of the security program. |
| 164.308(a)(1)(ii) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf | Implementation specifications for security management process | What are your organization's current and planned controls? Do you have them formally documented? | HIPAA Reg Met | No | N/A | Security controls are documented in the security diagrams of the scoped SOC 2 system. In addition, a Threat Analysis was conducted in April of 2024, which highlighted the controls that would reduce the impact of a vulnerability being exercised by a threat. |
| 164.308(a)(1)(ii) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf | Implementation specifications for security management process | Has your organization assigned responsibility to check all hardware and software, including hardware and software used for remote access, to determine whether selected security settings are enabled? | HIPAA Reg Met | No | N/A | ORGANIZATION uses a tool called Addigy to maintain an inventory of hardware and software. When connecting to the VPN, the device must have specific security controls before it can join the network. For example, Malware software must be present of the device will not be able to connect to systems the process ePHI. |
| 164.308(a)(1)(ii) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf | Implementation specifications for security management process | Does your organization have an analysis of current safeguards and their effectiveness relative to the identified risks? | HIPAA Reg Met | No | N/A | A Threat Analysis was conducted in April of 2024, which highlighted the controls that would reduce the impact of a vulnerability being exercised by a threat. Need to document the vulnerability process. |
| 164.308(a)(1)(ii) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf | Implementation specifications for security management process | Are any of your organization's facilities located in a region prone to any natural disasters, such as earthquakes, floods, or fires? Others? | HIPAA Reg N/A | N/A | N/A | All physical access is handled by Oracle OCI at the Oracle data centers. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Does your organization have policies and procedures in place for security? | HIPAA Reg Met | N/A | N/A | ORGANIZATION has policies and procedures in place for security. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Do your organization's current safeguards ensure the confidentiality, integrity, and availability of all ePHI? | HIPAA Reg Met | N/A | N/A | ORGANIZATION's current safeguards ensure the confidentiality, integrity, and availability of all ePHI. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Do your organization's current safeguards protect against reasonably anticipated uses and of ePHI that are not permitted by the HIPAA Privacy Rule? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is a business associate, which means the privacy rule does not apply to BA's. However, ORGANIZATION ensures that privacy is being implemented at a Covered Entity. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Has your organization protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION does conducted penetration testing from an outsourced third-party. In addition, ORGANIZATION runs vulnerability scans weekly against the PHI environment. Furthermore, ORGANIZATION has an MDR solutions to watch for threats to endpoints 24/7/365. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Does your organization have a formal and documented system security plan? | HIPAA Reg Met | No | N/A | ORGANIZATION has an ISMP with applicable documented policies, procedures and standards. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Will your organization's new security controls work with your organization's existing IT architecture? | HIPAA Reg Met | No | N/A | Security controls are evaluated in the Change Control process, as well as the ARB when the issues arise. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Does your organization have formal and documented contingency plan? | HIPAA Reg Met | Yes | High | ORGANIZATION does not have a clearly defined CP for its processes that has been evaluated and tested. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Does your organization have a communication plan or a process for communicating policies and procedures to your appropriate staff member, office and all your workforce? | HIPAA Reg Met | No | N/A | ORGANIZATION uses the all-hands meeting, Confluence, and email to communicate policies and standards. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Does your organization review and update your policies, procedures and standards as needed and when appropriate? | HIPAA Reg Met | No | N/A | The ORGANIZATION Information Security Progam Policy states that we need to update our policies at least annually for when a signifcant change happens. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Has your organization assured compliance with all policies and procedures by all your staff and workforce? | HIPAA Reg Met | No | N/A | ORGANIZATION assures compliance with all policies and procedures by all staff and workforce through a comprehenisive security awaresss program. |
| 164.308(a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a). | Your organization must implement sufficient security measures to reduce your risks and your vulnerabilities to a level that is both reasonable and appropriate level to comply with HIPAA Security. | Has your organization developed a training schedule for your Risk Management Program? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts it's risk management training at the CSPC on a bi-monthly basis reviewing the risk register and creating metrics to ensure trainin is appropriate. |
| 164.308(a)(1)(ii)(C) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | Your organization must implement appropriate sanctions against any and all of your staff and workforce members who fail to comply, by making a mistake or causing a harmful event, with your security policies, procedures or standards. | Does your organization have in place a formal and documented process, plus policy and procedures that address system misuse, abuse, and any fraudulent activities with your organization's ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION uses an Acceptable Use Policy that must be signed by all ORGANIZATION workers and non-workers. |
| 164.308(a)(1)(ii)(C) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | Your organization must implement appropriate sanctions against any and all of your staff and workforce members who fail to comply, by making a mistake or causing a harmful event, with your security policies, procedures or standards. | Has your organization made all your staff, employees, and workforce aware of your processes, policy and procedures (concerning sanctions for inappropriate access), use, disclosure, and transmission of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures workforce members are aware of policies and procedures via the Acceptable Use Policy (AUP). The AUP covers key components of each policy. Workforce members must sign that they received and understood the AUP. |
| 164.308(a)(1)(ii)(C) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | Your organization must implement appropriate sanctions against any and all of your staff and workforce members who fail to comply, by making a mistake or causing a harmful event, with your security policies, procedures or standards. | Do your organization's sanctions have a tiered structure of sanctions that takes into consideration the magnitude of harm to your organization and the individual whose ePHI is at risk, and the possible types of inappropriate disclosures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a clear Sanctions Policy that is managed by the People Team. The sanctions are a tiering process. |
| 164.308(a)(1)(ii)(C) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | Your organization must implement appropriate sanctions against any and all of your staff and workforce members who fail to comply, by making a mistake or causing a harmful event, with your security policies, procedures or standards. | Does your organization have a process, procedure or communication plan of how and when your managers and staff, employees and workforce will be notified of suspected inappropriate activity? | HIPAA Reg Met | No | N/A | ORGANIZATION has a clearly defined Incident Response Policy and Plan. The plan is communicated to applicable workforce members when needed. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | Does your organization have a formal, documented systems activity process and procedures? | HIPAA Reg Partially Met | Partial | Medium | ORGANIZATION has logs but those logs are not reviewed consistently. ORGANIZATION does have an Audit and Logging policy that system owners need to implement.   For endpoint management, ORGANIZATION has BitDefender MDR to monitor actives on endpoints.   Recommendation: Acquire and outsourced service for IaaS review of security logs and activity. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | Who, and which office/department, within your organization is responsible for overall systems activity process, procedures and results? | HIPAA Reg Met | No | N/A | IT & Engineering are responsible for overall systems activity process, procedures and results. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | How often does your organization review your information systems activity? What are the exceptions to the process that changes the review period? | HIPAA Reg Partially Met | No | N/A | ORGANIZATION production systems and endpoints are reviewed on a daily basis. There are no changes to the process at this time. However, log monitoring needs to be tightened up. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | How often does your organization analyze your systems activity reviews/reports? | HIPAA Reg Met | No | N/A | Daily, However, log monitoring needs to be tightened up. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | Does your organization review exception reports and logs? | HIPAA Reg Met | No | N/A | Exceptions reports are reviewed during a change control request to make changes based on logs. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | What mechanisms and measures will your organization implement to assess the effectiveness of your review process? | HIPAA Reg Partially Met | Partial | Medium | ORGANIZATION uses a tool called Data Dog to capture production logs. However, the security log reviews of the production systems need to be tightened up. Endpoints are covered by BitDefender and Addigy, as well as Apple MDM. |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | Does your organization file, electronic and/or paper, monitoring reports, and how are these reports monitored? | HIPAA Reg Met | No | N/A | ORGANIZATION has logging but monitoring is lacking |
| 164.308(a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Your organization must implement procedures to regularly review your records of your information system activity, including audit logs, access reports, security incident report, and any other document used by your organization. | Does your organization have a sanction policy for staff, employee or workforce violations? | HIPAA Reg Met | No | N/A | ORGANIZATION has a clear Sanctions Policy that is managed by the People Team. The sanctions are a tiering process. |
| 164.308(a)(2) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | Your organization must identify, and name, the security official who is responsible for the development and implementation of your HIPAA Security policies and procedures. | Does your organization have a complete security official job description that accurately reflects the security duties and responsibilities? Does it include all areas outlined and spoken of in the questions outlined for this security standard? | HIPAA Reg Met | No | N/A | ORGANIZATION has a full time Compliance, Security, and Privacy officer. The official has a BAA in Information Security Management, an MS in Information Assurance, a CISSP, ISSMP, CDPSE, and CCSFP. The official has 23+ year’s experience in the domain. |
| 164.308(a)(2) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | Your organization must identify, and name, the security official who is responsible for the development and implementation of your HIPAA Security policies and procedures. | Have all your organization's staff, employees, workforce, offices and departments been notified of the name and office to contact with a security problem? | HIPAA Reg Met | No | N/A | ORGANIZATION's CTO has communicated to all staff at the beginning of the Officials role beginning. The CTO states who the official is on server all-hand meetings. The Official also conducts training and lunch and learns. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization implemented procedures for authorization and/or supervision of work force members who work with ePHI or in locations where it might be accessed? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures workforce members have least privilege access. Access is authorized by workforce members manager/supervisor. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization defined roles and responsibilities for all job functions? | HIPAA Reg Partially Met | Yes | Medium | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs led to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Have staff members been provided copies of their job descriptions, informed of the access granted to them, as well as the conditions by which this access can be used? | HIPAA Reg Partially Met | Yes | Medium | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs led to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Does your organization have a listing in **writing** who has the business need, and who has been granted permission, to view, alter, retrieve, and store ePHI, and at what times, and under what circumstances and for what purposes? | HIPAA Reg Partially Met | Yes | Medium | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs lead to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Does your organization have written job descriptions that are correlated with appropriate levels of access? | HIPAA Reg Not Met | Yes | High | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs lead to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Does your organization have an established set of qualifications for each job description? | HIPAA Reg Not Met | Yes | High | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs lead to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Does your organization check a candidate's qualifications against a specific job description? | HIPAA Reg Partially Met | Yes | Medium | Job descriptions help identify particular skills or abilities that are necessary for a given position or the environmental pressures that apply to the position. A good job description tells the applicant what is required for the role. JDs lead to position expectations and should be clearly discussed with the candidates. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization made a determination of each candidate for a specific position can perform the tasks for that position? | HIPAA Reg Met | No | N/A | ORGANIZATION posts jobs to a tool called Lever. Specific job requirements are posted for candidates to review. Interviews |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization established chains or command and lines of authority for workforce security? | HIPAA Reg Met | No | N/A | ORGANIZATION has established organizational charts and lines of authority for workforce security located in BambooHR. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization established a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations and personnel? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION does not have any physical workforce facilities. |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization made your work staff aware of the identity and roles of their supervisors? | HIPAA Reg Met | No | N/A | Brandon? |
| 164.308(a)(3)(A) | 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. | Your organization must develop and implement procedures for authorization and/or supervision of staff, employees, and workforce members who work with ePHI or in locations where it may be accessed. | Has your organization provided staff, employees, and workforce members with a copy of their job descriptions, informed of the access granted to them, as well as the conditions by which this access can be used? | HIPAA Reg Met | No | N/A | Brandon? |
| 164.308(a)(3)(B) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Your organization needs to implement procedures to determine that access of one of your staff, employees, or workforce members to ePHI is appropriate, and meets the policies and procedures outlined above. | Does your organization check an applicant's employment and educational references, if this is reasonable for such a job description? | HIPAA Reg Met | No | N/A | Brandon? |
| 164.308(a)(3)(B) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Your organization needs to implement procedures to determine that access of one of your staff, employees, or workforce members to ePHI is appropriate, and meets the policies and procedures outlined above. | Does your organization do background checks, such as a Criminal Offender Record Information (CORI) check, if appropriate in the circumstances? | HIPAA Reg Partially Met | Yes | Medium | ORGANIZATION needs to implement a comprehensive background check program that includes ALL workforce member; employees and non-employees. |
| 164.308(a)(3)(B) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Your organization needs to implement procedures to determine that access of one of your staff, employees, or workforce members to ePHI is appropriate, and meets the policies and procedures outlined above. | Does your organization have a process and strategy that supports your organizations authorizes who are permitted to designate and grant access to ePHI? | HIPAA Reg Met | No | N/A | Brandon? |
| 164.308(a)(3)(B) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Your organization needs to implement procedures to determine that access of one of your staff, employees, or workforce members to ePHI is appropriate, and meets the policies and procedures outlined above. | Does your organization have formal and documented procedures for obtaining the necessary and appropriate signoffs within your organizational structure to both grant and terminate access to ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has an access Control policy that implements least privilege to ePHI. Users are authorized by their managers to get access via a Jira ticket, and removal of access when necessary. |
| 164.308(a)(3)(C) | Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | Your organization must have procedures for terminating, stopping, access of ePHI by staff, employees and workforce members when they are no longer an employee, student or volunteer. | Does your organization have standards set of procedures to recover access control devices, including identification badges, keys access cards from staff, employees and workforce member where their employment ends? | HIPAA Reg N/A | N/A | N/A | This control has to do with physical access. ORGANIZATION is 100% remote organization. |
| 164.308(a)(3)(C) | Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | Your organization must have procedures for terminating, stopping, access of ePHI by staff, employees and workforce members when they are no longer an employee, student or volunteer. | Does your organization have a procedure to deactivate computer, and other electronic tools, access accounts, including the process that will disable user IDs and passwords? | HIPAA Reg Met | N/A | N/A | ORGANIZATION has an access Control policy that implements least privilege to ePHI. Users are authorized by their managers to get access via a Jira ticket, and removal of access when necessary. |
| 164.308(a)(3)(C) | Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | Your organization must have procedures for terminating, stopping, access of ePHI by staff, employees and workforce members when they are no longer an employee, student or volunteer. | Does your organization need, and have separate termination procedures for voluntary termination, including retirement, promotion, transfer, or change of employment internal to your organization, versus involuntary termination, including for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions? | HIPAA Reg Met | No | N/A | ORGANIZATION has separate termination procedures for voluntary termination, including retirement, promotion, transfer, or change of employment internal to your organization, versus involuntary termination, including for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions |
| 164.308(a)(3)(C) | Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | Your organization must have procedures for terminating, stopping, access of ePHI by staff, employees and workforce members when they are no longer an employee, student or volunteer. | Does your organization have a standard checklist of action items for completion when a staff, employee, workforce member leaves your employment, such a s the return of all access devices, deactivation of logon accounts, including remote access, and return of any computers and other similar electronic tools, such as a PDA, and cell phone, and delivery of any data/information under this staff, employee of workforce member control? | HIPAA Reg Met | N/A | N/A | ORGANIZATION's IT department has a checklist to remove access and collect applicable assets. |
| 164.308(a)(3)(i) | 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. | Your organization must implement policies and procedures to ensure that any and all staff, employees, and workforce members have appropriate, and only appropriate, access to ePHI; and to prevent the staff, employees, and workforce members who do not have access to ePHI from obtaining access to ePHI. | Has your organization implemented policies and procedures to ensure that any and all staff, employees, and workforce members have appropriate, and only appropriate, access to ePHI; and to prevent the staff, employees, and workforce members who do not have access to ePHI from obtaining access to ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has an Access Control policy that implements least privilege to ePHI. Users are authorized by their managers to get access via a Jira ticket. |
| 164.308(a)(4)(i) S | 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. | Your organization must implement policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI. | Has your organization implemented policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI? | HIPAA Reg Met | N/A | N/A | ORGANIZATION has implemented policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI through a comprehensive access control policy, procedure and process |
| 164.308(a)(4)(ii) | Implement policies and procedures that protect the electronic protected health information from unauthorized access by the larger organization. | Information access management | Has your organization reviewed the isolating clearinghouse functions implementation specifications? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Does your organization have a component that functions as a healthcare clearinghouse? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Has your organization a formal and documented finding that one part of your organization is a healthcare clearinghouse? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Has your organization healthcare clearinghouse developed and implemented policies and procedures that protect the clearinghouse ePHI form unauthorized access by the other parts of your organization? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Does your organization's clearinghouse share hardware or software with your larger organization of which it is part? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Does your organization's clearinghouse share staff or physical space with staff from a larger organization? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Has your organization established a separate network or subsystem for your organization's clearinghouse? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | This implementation specification only applies if you are a complex enterprise and are more than a clearinghouse and have clearinghouse functions as part of your organization. If a healthcare clearinghouse is part of your larger organization, you must implement this requirement. | Has your organization's clearinghouse staff, employees, and workforce been trained to safeguard ePHI from disclosure to your larger organization? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION is not a clearing house |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Has your organization formally documented how access to ePHI will be granted to your staff, employees, and workforce members? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI through a comprehensive access control policy, procedure and process |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Has your organizations formally documented the basis for restricting access to ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI through a comprehensive access control policy, procedure and process |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Has your organization formally documented your ePHI access control method? Does your organization use identity-based, role-based, biometric based, proximity based, other means of access, or a combination of access | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented policies and procedures that authorized your staff, employees and workforce to access to ePHI to provide protection for the use and disclosure of the ePHI through a comprehensive access control policy, procedure and process |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization's job descriptions accurately reflect assigned duties, responsibilities and enforcement of segregation of duties? | HIPAA Reg Met | Yes | Low | ORGANIZATION has job descriptions that reflect assigned duties, responsibilities, however there is not a clearly documented part on enforcement of segregation of duties? |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization grant your staff, employees and workforce members remote access to ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION Does grant employees and workforce members remote access to ePHI via the access control process. Least privilege is strictly enforced. |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees, and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Has your organization determined if direct access to ePHI will be granted to third parties external to your organization, including business partners, other providers, health plans, patients, and members to their own ePHI, and others? | HIPAA Reg Met | No | N/A | ORGANIZATION Does grant third-party members remote access to ePHI via the access control process. Least privilege is strictly enforced. |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization's IT systems have the capacity to set access controls? | HIPAA Reg Met | No | N/A | ORGANIZATION Does grant third-party members remote access to ePHI via the access control process. Least privilege is strictly enforced. |
| 164.308(a)(4)(ii)(B) | 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. | Your organization needs to implement policies and procedures to grant access to your staff, employees and workforce members to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization use stronger access controls for sensitive data? | HIPAA Reg Met | No | N/A | ORGANIZATION has encyption specifically for ePHI. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Has your organization formally documented the standards you use to grant a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms? | HIPAA Reg Met | No | N/A | ORGANIZATION has formal documented standard granting workforce access to workstations and applicable systems. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization have security access controls policies and procedures? Are they updated regularly? | HIPAA Reg Met | No | N/A | ORGANIZATION has formal documented standard granting workforce access to workstations and applicable systems. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization provide formal written and documented authorization from the appropriate manager before granting access to sensitive information? | HIPAA Reg Met | No | N/A | ORGANIZATION has formal documented standard granting workforce access to workstations and applicable systems. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Are your organization's staff, employees, and workforce member's duties separated so that only the minimally necessary ePHI based on the specific job description is made available upon request? | HIPAA Reg Met | No | N/A | ORGANIZATION has formal documented separation of duties policy and standard. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization have authentication mechanisms to verify the identity of the user accessing the system? | HIPAA Reg Met | No | N/A | ORGANIZATION uses MFA to ensure the indentity of the workforce member. |
| 164.308(a)(4)(ii)(C) | 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, program, or process. | Your organization needs to develop and implement policies and procedures based on your organization's access authorization that establish, document, review, an modify a staff, employee, workforce member user's access to a workstation, laptop, transaction, program, process, and other tools and mechanisms. | Does your organization's management regularly review the list of access authorizations, including remote access authorizations, to verify that the list is accurate and has not been inappropriately altered? | HIPAA Reg Partially Met | Partial | Medium | Do we have a formal proces for this control? |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization formally determined and documented your security training needs? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization interview key staff when assessing your security training needs? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Did your organization's assessment include the security training needs of sensitive data, and other similar information? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization determined what awareness, training and education programs are needed, and which programs will be required? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization outlined content and audience training priorities? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | What gaps did your organization discover in conducting the training assessment; outline what needs to be added and updated? | HIPAA Reg Met | No | Medium | When ORGANIZATION identifies issues they are identifed in security awarness training for future events |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include an outline of your organization's specific policies and procedures that require security awareness and training? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented a Workforce Education and Awareness Training Policy that is implemented via security awareness platform. The platform ensures the training strategy and plan include an outline of your ORGANIZATION's policies and procedures requiring security awareness and training. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include scope of the awareness an training program? | HIPAA Reg Met | No | N/A | ORGANIZATION createsannual awareness training. The scope is based on job role/ |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the goals? | HIPAA Reg Met | No | N/A | ORGANIZATION has targeted goals. For example, we target phishing testing below industry percentages. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the target audience(s)? | HIPAA Reg Met | No | N/A | ORGANIZATION has targeted goals. For example, we target phishing testing below industry percentages. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the learning objectives? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool and determined by quarter. Each learning objective is documented in Mooncamp and discussed at the CSPC. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the deployment methods? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool and determined by quarter. Each learning objective is documented in Mooncamp and discussed at the CSPC. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include evaluation of the training through designated measurement techniques? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool and determined by quarter. Each learning objective is documented in Mooncamp and discussed at the CSPC. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the frequency of training? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool and determined by quarter. Each learning objective is documented in Mooncamp and discussed at the CSPC. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's training strategy and plan include the consideration of compliance dates and the HITECH Act Updates? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization have a process, a procedure, in place to ensure that everyone in your organization receives security awareness training? | HIPAA Reg Met | No | N/A | ORGANIZATION has an awareness and training policy and procedure to ensure that all workforce members receive training. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization have a plan in place to for training to address specific technical topics based on job descriptions and responsibilities? | HIPAA Reg Met | No | N/A | ORGANIZATION creates annual awareness training. The scope is based on job role/ |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization train your non-employees, such as contractors, interns, volunteers, and others? | HIPAA Reg Met | No | N/A | ORGANIZATION has an awareness and training policy and procedure to ensure that all workforce members receive training. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization selected topics to be included in your training content, materials and methods? | HIPAA Reg Met | No | N/A | Learning objectives are taken from the KnowBe4 tool and determined by quarter. Each learning objective is documented in Mooncamp and discussed at the CSPC. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization incorporate new information from email advisories, daily news web sites, periodical, and other sources into your training content and materials when reasonable and appropriate? | HIPAA Reg Met | No | N/A | ORGANIZATION uses Feedly to stay up to date with current news. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | What and how many different types of media and venues does your organization use for security awareness training; such as computer based training, on-site trailing, electronic and paper publications, others; name them? | HIPAA Reg Met | No | N/A | ORGANIZATION reviews 25 news sources. In addition, ORGANIZATION uses KnowBe4 for training when ORGANIZATION identifies a weakness for threat (e.g., phishing) |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization given each staff, employee, and workforce member a copy of your security polices and procedures, and do they know where to find them on your internal web or server or other place? | HIPAA Reg Met | No | N/A | Upon new hire, workforce members are introduced to the policies and procedures. Workforce members also are required to sign the AUP, which is a summary of all the policies. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Do your organization's staff, employees, workforce members know whom to contact and the procedures to handle a security incident? | HIPAA Reg Met | No | N/A | ORGANIZATION's workforce members are told where to report events. The communication is sent via All Hands and Slack Comms. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's staff, employees, workforce members know and understand the consequences of their noncompliance with your organization's security policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a sanctions policy describing consequences for actions. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization's staff, employees, workforce members know how to handle physical security and information security issues with a laptop, PDA, tablet, smart phone, and/or other similar tools? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION ensures staff, employees, workforce members know how to handle physical security and information security issues with a laptop, tablets, smart phone, and/or other similar tools |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization continuously research security issues and security training? Do you update your security training content, materials and evaluation with the new information? | HIPAA Reg Met | No | N/A | ORGANIZATION uses Feedly to stay up to date with current news and updates training based on risk and threats. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Has your organization scheduled and conducted the training outlined in your training strategy and plan and how often has your organization done security training since the publication of the HIPAA Security Rule? | HIPAA Reg Met | No | N/A | ORGANIZATION does training at least annually |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization have sanctions to impose on staff, employees and workforce if they do not complete the required security training? | HIPAA Reg Met | No | N/A | ORGANIZATION has a sanctions policy describing consequences for actions. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization keep your security awareness and training program current by updating it periodically? What is the review and update period? | HIPAA Reg Met | No | N/A | ORGANIZATION keeps their awareness training up to date using a tool called KnowBe4. Reviews and update periods are annual. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization conduct new or additional security training whenever changes occur in either technology or practices? | HIPAA Reg Met | No | N/A | ORGANIZATION keeps their awareness training up to date using a tool called KnowBe4. Reviews and update periods are annual. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization have a new hire security awareness, technology and information systems training plan? | HIPAA Reg Met | No | N/A | Upon new hire, workforce members are introduced to the policies and procedures. Workforce members also are required to sign the AUP, which is a summary of all the policies. |
| 164.308(a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | Your organization must determine the security training needs of your organization and then develop and implement a security awareness and training program for all staff, employees and workforce members including all of your management. | Does your organization train non-employees, including, contracts/vendors, interns, volunteers, and others? | HIPAA Reg Met | No | N/A | Upon new hire, workforce members are introduced to the policies and procedures. Workforce members also are required to sign the AUP, which is a summary of all the policies. |
| 164.308(a)(5)(ii) | Implement procedures for periodic security updates, guarding against, detecting, and reporting malicious software, monitoring log-in attempts and reporting discrepancies, and creating, changing, and safeguarding passwords. | Your organization must determine the frequency of security updates, how to guard against, detect, and report malware, how to monitor log-in attempts and report discrepancies, and how to create, change, and safeguard passwords. | Do employees know the importance of timely application of system patches to protect against malicious software and exploitation of vulnerabilities? | HIPAA Reg Met | No | N/A | ORGANIZATION's IT department uses automated tools to update mobile devices, including laptops. |
| 164.308(a)(5)(ii) | Implement procedures for periodic security updates, guarding against, detecting, and reporting malicious software, monitoring log-in attempts and reporting discrepancies, and creating, changing, and safeguarding passwords. | Your organization must determine the frequency of security updates, how to guard against, detect, and report malware, how to monitor log-in attempts and report discrepancies, and how to create, change, and safeguard passwords. | Are employees aware that log-in attempts may be monitored? | HIPAA Reg Met | No | N/A | ORGANIZATION does not have a logon banner stating that the ORGANIZATION-device is owned by ORGANIZATION and that there is no expectation of privacy on ORGANIZATION-Owned devices. |
| 164.308(a)(5)(ii) | Implement procedures for periodic security updates, guarding against, detecting, and reporting malicious software, monitoring log-in attempts and reporting discrepancies, and creating, changing, and safeguarding passwords. | Your organization must determine the frequency of security updates, how to guard against, detect, and report malware, how to monitor log-in attempts and report discrepancies, and how to create, change, and safeguard passwords. | Do employees that monitor log-in attempts know to whom to report discrepancies? | HIPAA Reg Met | No | N/A | ORGANIZATION's workforce members are told where to report events. The communication is sent via All Hands and Slack Comms. |
| 164.308(a)(5)(ii) | Implement procedures for periodic security updates, guarding against, detecting, and reporting malicious software, monitoring log-in attempts and reporting discrepancies, and creating, changing, and safeguarding passwords. | Your organization must determine the frequency of security updates, how to guard against, detect, and report malware, how to monitor log-in attempts and report discrepancies, and how to create, change, and safeguard passwords. | Do employees understand their roles and responsibilities in selecting a password of appropriate strength, changing the password periodically (if required), and safeguarding their password? | HIPAA Reg Met | No | N/A | ORGANIZATION has password policies that instruct users on how to make good passwords. In addition, password creation is configured in the MDM solution to ensure good passwords are made meeting password requirements. |
| 164.308(a)(5)(ii)(A) | Periodic security updates. | Your organization needs to provide periodic security mini-training through alerts, briefings and training updates when HIPAA Security law, regulations and guidance is updated | Does your organization provide periodic security updates to your staff, employees, workforce, business associates and contractors/vendors? | HIPAA Reg Met | No | N/A | ORGANIZATION has all hands meetings where workforce members are updated on current security updates. |
| 164.308(a)(5)(ii)(A) | Periodic security updates. | Your organization needs to provide periodic security mini-training through alerts, briefings and training updates when HIPAA Security law, regulations and guidance is updated | What methods does your organization already have in place or use to keep your staff, employees, workforce, business associates and contractors/vendors updated and aware of security other ways? | HIPAA Reg Met | No | N/A | ORGANIZATION uses Feedly to stay up to date with current news and updates training based on risk and threats. |
| 164.308(a)(5)(ii)(A) | Periodic security updates. | Your organization needs to provide periodic security mini-training through alerts, briefings and training updates when HIPAA Security law, regulations and guidance is updated | Does your organization provide security awareness training with all new hires before they are given access to ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION provides all new workforce members with security training prior to start of work. |
| 164.308(a)(5)(ii)(B) | Procedures for guarding against, detecting, and reporting malicious software. | As reasonable and appropriate, train employees regarding procedures for: Guarding against, detecting, and reporting malicious software; Monitoring log-in attempts and reporting discrepancies; and Creating changing, and safeguarding passwords. Incorporate information concerning staff members’ roles and responsibilities in implementing these implementation specifications into training and awareness efforts. | Has your organization trained your staff, employees, and workforce members in procedures for... \* Guarding against, detecting, and reporting malicious software \* Monitoring log-in attempts and reporting discrepancies \* Creating changing and safeguarding passwords? | HIPAA Reg Met | No | N/A | ORGANIZATION provides all new workforce members with security training prior to start of work. |
| 164.308(a)(6)(i) | Implement policies and procedures to address security incidents. | Your organization must develop and implement policies and procedures to any security incidents. A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or the interference with system operations in an information system | Has your organization implemented policies and procedures for any security incidents? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented an incident security policy. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization documented incident response procedures that can provide your organization with a single point of reference to guide the day-to-day operations of the incident response team? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented an incident security policy and procedure. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization determined how it will respond to a security incident? Are there a formal documented policy and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented an incident security policy and procedure. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization incorporated your staff, employee, workforce members jobs and job descriptions roles and responsibilities in \* Guarding against, detecting, and reporting malicious software, \* Monitoring log-in attempts and reporting discrepancies \* Creating changing and safeguarding password in your security awareness training efforts? | HIPAA Reg Met | No | N/A | All of these controls are handled by ORGANIZATION's IT department through automated controls. For example, BitDefender for malware. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization reviewed incident response procedures with the staff, employees, or workforce members with the roles and responsibilities related to incident response, solicit suggestions for improvement, and make changes to reflect input that is reasonable and appropriate? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts Tabletop Exercises with appropriate personnel. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization monitor log-in attempts? Do your staff, employees and workforce members know of this monitoring? | HIPAA Reg Not Met | Yes | Low | ORGANIZATION should have a logon banner that states that login attempts are monitored. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization analyzed these problems and created a mitigation plan that it is working to decrease risks and vulnerabilities? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts vulnerability scanning and pen testing to ensure threats and vulnerabilities are identified and mitigated based on risk. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization have a process, procedure for reporting and handling security incidents? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented an incident security policy and procedure. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization prioritized your key functions to determine what would need to be restored first in the event of a disruption? | HIPAA Reg Met | No | N/A | ORGANIZATION's disaster recovery relies on the OCI environment. ORGANIZATION ensures that backups are executed timely. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization update the incident response procedures when your organizational needs change? | HIPAA Reg Met | No | N/A | All ORGANIZATION's policies and procedures are updated at least annually, or when a significant change happens requiring updating. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization told your staff, employees and workforce members how to and where to report a security incident? | HIPAA Reg Met | No | N/A | ORGANIZATION has implemented an incident security policy and procedure. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization developed standard incident reporting templates to ensure that all necessary information related to an incident is documented and investigated? | HIPAA Reg Met | No | N/A | ORGANIZATION has a SIRT process implemented in Jira to report alerts, events, and possible incidents. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | If you have determined that your organization does not need a standing incident response team, what other response mechanism are you using? | HIPAA Reg Met | No | N/A | ORGANIZATION has a SIRT team made up of various individuals across the orgnization to include the CPSC. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization determine what information and when data will be disclosed to the media? | HIPAA Reg Met | No | N/A | ORGANIZATION will communicate what is necessary per the HIPAA Security Rule requirements. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization have an identified list of both internal and external persons and their contact information who should be informed of a security incident has occurred? | HIPAA Reg Met | No | N/A | ORGANIZATION maintains a list of necessary individuals for the SIRT. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization have mitigation options for security incidents? | HIPAA Reg Met | No | N/A | ORGANIZATION uses the PIR process to mitigate issues. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Do your organization's staff, employees, and workforce members know where and to whom to report log-in discrepancies? | HIPAA Reg Met | No | N/A | ORGANIZATION staff can report issues via the IT Support slack channel. #it-support. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization named an individual, or several individuals, to speak for your organization to the media, law enforcement, clients, business partners and others? | HIPAA Reg Met | No | N/A | ORGANIZATION has a designated individual to communicate to external partners. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Do your organization's staff, employees, and workforce members understand their roles and responsibilities in selecting a password of appropriate strength, changing the password periodically as required, and safeguarding their password? | HIPAA Reg Met | No | N/A | ORGANIZATION workforce are training on how to come up with a good password. There are technical controls in place to prevent bad passwords. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization review your current procedures and determine if they were adequate and appropriate to respond to this particular security incident? And make updates and changes as necessary? | HIPAA Reg Met | No | N/A | ORGANIZATION has an information security incident response procedure. Roles have been defined. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization's incident response team or individual keep documentation of security incidents, their outcomes, including weaknesses exploited and how access to information was gained? | HIPAA Reg Met | No | N/A | ORGANIZATION has an information security incident response procedure. Roles have been defined. Outcomes go into the SIRT Jira site. Any issues found are put into the ORGANIZATION Risk Register. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Does your organization employ malicious code protection mechanisms at information system entry and exit points and at workstations servers, or mobile computing devices on the network to detect and eradicated malicious code) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means? | HIPAA Reg Met | No | N/A | ORGANIZATION uses BitDefender on all mobile endpoints. ORGANIZATION uses Paubox for email malicious code detection. |
| 164.308(a)(6)(ii) | Response and Reporting (Required). 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; and document security incidents and their outcomes. | Security incident procedures | Has your organization determine what information and when data will be disclosed to the media? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures that any information exposed to the media is handled by customer care. |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization established your organization's contingency plan framework, roles and responsibilities? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization's contingency policy and plan address scope, resource requirements, training, testing, plan maintenance and backup requirements? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization's policy and plan outline what critical services must be provided within specific timeframes? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization's policy and plan identify and outline cross-functional dependencies to determine how failure in one systems impacts other system(s)? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization outlined scenarios and identified preventive measures, measures you can do now, for each scenario that could result in the loss of a critical service involving the use of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts Tabletop Exercises with appropriate personnel. |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization brain stormed and outlined alternatives for continuing operations for your organization if you lose a critical function or a critical resource? Remember there are physical resources like offices and desks and copiers and paper, electronic recourses, computers, and servers. a connection to the Internet and phones, and human resources. Have you brainstormed what Human Resources need if they are going to do manual chores instead of electronic chores and are going to operate 24/7? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has you organization researched the cost of preventive measures being considered? | HIPAA Reg Met | No | N/A | ORGANIZATION's RLT and Finance reviews preventive measure costs, like Cyber-Insurance |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Are the preventable measures you are considering affordable and practical for the environment? | HIPAA Reg Met | No | N/A | ORGANIZATION reviews software fees to ensure they are adequate for preventive controls. The reviews are conducted by Finance. |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization have an emergency coordinator who manages, maintains and updates the contingency plan? Does your organization's staff, employees, and workforce members know who this individual is and how to contact your coordinator? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization have an emergency call list? Has it been distributed to all staff, employees, and workforce members? | HIPAA Reg Not Met | Yes | High | ORGANIZATION needs to develop and emergency call list |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization have a determination of when your contingency plan needs to be activated? Is it triggered by anticipated duration of outage, loss of capability, or impact on service delivery? Other? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization have plans, procedures, and agreements initiated or in place if the preventive measures need to be implemented? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization finalized a set of contingency procedures that can be invoked for all identical impacts, including emergency mode of operation? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(i) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Does your organization have documented procedures related to recovery from emergency or disastrous events? | HIPAA Reg Met | N/A | N/A | ORGANIZATION's outsourced infrastructure team has ownership on the disaster recovery. |
| 164.308(a)(7)(i) | 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization reviewed the data backup plan and disaster recovery plan implementation specifications? | HIPAA Reg Partially Met | Yes | Medium | Backup testing is informally done. Backups are restored as needed but nothing formal to test. |
| 164.308(a)(7)(ii) | 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. | Your organization must have policies and procedures to respond to an emergency and other adverse events that could potentially damage systems that control ePHI. | Has your organization reviewed the data backup plan and disaster recovery plan implementation specifications? | HIPAA Reg Partially Met | Yes | Medium | Backup testing is informally done. Backups are restored as needed but nothing formal to test. |
| 164.308(a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Your organization needs a plan and procedures to keep and be able to receive exact copies of your ePHI. | Does your organization's contingency plan address disaster recovery and back up? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Your organization needs a plan and procedures to keep and be able to receive exact copies of your ePHI. | Has your organization established and implemented procedures to create and maintain retrievable exact copies of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION's outsourced infrastructure team has ownership on the disaster recovery. |
| 164.308(a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Your organization needs a plan and procedures to keep and be able to receive exact copies of your ePHI. | Has your organization established and implemented procedures to restore any loss of ePHI? | HIPAA Reg Met | No | N/A | Do ORGANIZATION have procedures to restore backups? |
| 164.308(a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Your organization needs a plan and procedures to keep and be able to receive exact copies of your ePHI. | Has your organization documented all your data backup procedures and made them available to all your staff, employees, and workforce members? | HIPAA Reg Met | No | N/A | Do ORGANIZATION have procedures to restore backups? |
| 164.308(a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Your organization needs a plan and procedures to keep and be able to receive exact copies of your ePHI. | Does your organization have individuals/office named and responsibilities assigned to conduct backup activities? | HIPAA Reg Met | No | N/A | Do ORGANIZATION have procedures to restore backups? |
| 164.308(a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | "Emergency mode" operations involves only the critical business processes that must occur to protect the security of ePHI during and immediately after the crisis situation. | Has your organization established, and implemented when needed, procedures to enable continuation of critical business processes for the security of ePHI while your organization is operating in emergency mode? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | "Emergency mode" operations involves only the critical business processes that must occur to protect the security of ePHI during and immediately after the crisis situation. | Has your organization identified your key activities and developed procedures to continue these key activities during an emergency? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | "Emergency mode" operations involves only the critical business processes that must occur to protect the security of ePHI during and immediately after the crisis situation. | Has your organization identified critical functions that use ePHI? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | "Emergency mode" operations involves only the critical business processes that must occur to protect the security of ePHI during and immediately after the crisis situation. | During the emergency would different staff/employees, facilities or systems be needed to perform these critical functions during the emergency? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | "Emergency mode" operations involves only the critical business processes that must occur to protect the security of ePHI during and immediately after the crisis situation. | Can your organization assure the security of the ePHI in the alternative mode(s) operation? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization established and implemented as needed periodic testing procedures and for the revision of your organization's contingency plan? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization tested its contingency plan on a predefined cycle? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization trained your staff/employees with defined plan responsibilities in their roles? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Does your organization include external entities, including vendors, alternative site and service providers, in your testing exercises? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization determined how the plan will be tested? Will it be a Tabletop exercise, or a real operational scenario? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization determined how the plan will be tested? Will it be a Tabletop exercise, or a real operational scenario? | HIPAA Reg Met | N/A | N/A | ORGANIZATION does walk-throughs and Tabletop execises to identify any risks. |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Does your organization test during normal business hours? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Or must testing take place during off hours? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | How frequently does your organization test its plan? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | One of the baseline activates your organization needs to so is over time test and revise your contingency plan; technology changes, your services may change, your physical space may be updated or your may move. | Has your organization a timeline on when the contingency plan should be revised? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization identified the critical services or operations, and the manual and automated processes that support them, involving ePHI? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization determined what hardware and software and personnel are critical to your organization's daily business operations? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization determined the impact on desired service levels if these critical assets are not available? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization outlined the nature and degree of impact on your operations if any of the critical resources are not available? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization determined the amount of time your organization can tolerate disruption to these operations, material or services? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization determine what, if any, support is or can be provided by external providers, including ISPs, utilities, or contractors? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Your organization needs to identify all your activities and materials involving ePHI that are critical to your business. | Has your organization established cost-effective strategies for recovering these critical services, resources, or processes? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization have any existing reports or documentation that you had previously prepared or created by your organization addressing compliance, integration, or maturity of a particular or many security safeguard(s) deployed to protect ePHI that your can leverage for this evaluation? | HIPAA Reg Met | No | N/A | ORGANIZATION has a comprehensive Information Security & Privacy Policies that have been vetted by an external auditor. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization established a frequency for security evaluations, and disseminated this information to your entire organization? | HIPAA Reg Met | No | N/A | ORGANIZATION has a comprehensive Information Security & Privacy Program that have been vetted by an external auditor. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization's security policies specify that security evaluations will be repeated when environmental and operational changes, such as technology updates, are made that affect the security of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has a comprehensive Information Security & Privacy Program that have been vetted by an external auditor. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization's frequency of security evaluation policies reflect any and all federal laws, regulations, and guidance documents that impact environmental or operational changes affecting the security of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts security evaluations annually. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization's corporate, legal, and regulatory compliance staff, employees, or workforce members participate when you conduct your analysis? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts security evaluations annually to include RLT and Compliance. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization considered management, operational, and technical issues in your evaluation? | HIPAA Reg Met | No | N/A | ORGANIZATION has considered management, operational, and technical issues in the annual audits and assessments. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization performed a periodic technical and nontechnical evaluation, based initially upon the standards implemented? | HIPAA Reg Met | No | N/A | ORGANIZATION performs periodic technical and nontechnical vulnerability scanning. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization decided if your evaluation will be conducted by your internal staff and resources or by external consultants, or by a combination of internal and external resources? | HIPAA Reg Met | No | N/A | ORGANIZATION executes assessments from internal staff, doing risk assessments and vulnerability/threat scanning, and external staff to audit the overall security and privacy program. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Do any of your organization's staff, employee or workforce members have the technical experience to evaluate your systems? | HIPAA Reg Met | No | N/A | ORGANIZATION's compliance, IT, and engineering staff has the technical experience to evaluate your systems |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Do your staff, employees, or workforce members have the training necessary on security technical and non-technical issues? | HIPAA Reg Met | No | N/A | ORGANIZATION's compliance, IT, and engineering staff has the technical experience to evaluate your systems |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization outlined the necessary factors to be considered in selecting an outside vendor, including credentials and experience? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance conducts vendor due diligence to ensure the vendor is credible. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization use a strategy and tool that considers all the elements of the HIPAA Security Rule, including all standards and implementation specifications? | HIPAA Reg Met | No | N/A | ORGANIZATION has a roadmap that includes the 2-3 year strategy that includes applicable HIPAA Security Rule. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Do the elements of each of your organization's evaluation procedure, including questions, statement and other components, address individual, measurable security safeguards of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION executes an annual HIPAA Risk assessment that reviews safeguards with respect to HIPAA Security regulations. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization determined which security procedures must be tested in more than one system? | HIPAA Reg Met | No | N/A | ORGANIZATION uses the ORGANIZATION Decision Support system. This system is the system that is reviewed the most using existing procedures. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization determined in advance what departments and staff, employees, and/or workforce members will participate in your security evaluation? | HIPAA Reg Met | No | N/A | ORGANIZATION has determined the applicable groups for conduct audits, assessment and certifications. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization have senior management support for your security evaluation, and have they stated the need for everyone within your organization to participate in and support your security evaluation? | HIPAA Reg Met | No | N/A | ORGANIZATION RLT is fully committed to the information security and privacy program. Any assessments are brought to the CSPC for review and action planning, |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization included staff, employees, or workforce members with IT knowledge in your security evaluation team and used during your evaluation? | HIPAA Reg Met | No | N/A | ORGANIZATION has the applicable individuals to assist in any evaluation of the organization. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization collected and documented all information needed for your security evaluation, by interviews, surveys, and output of automated tools, for example, audit logging tools, results of penetration testing? | HIPAA Reg Met | No | N/A | ORGANIZATION completed their SOC 2 Report, which collected control evidence to support the SOC evaluation. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization conducted penetration testing? Before the penetration testing did your organization have management approval for such testing? | HIPAA Reg Met | No | N/A | ORGANIZATION conducts annual penetration testing. All pen testing has to be approved by the CSPC. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization formally communicated your security evaluation process to your staff, employees, and workforce members who have assigned roles and responsibilities in your evaluation process? | HIPAA Reg Met | No | N/A | ORGANIZATION has the applicable individuals to assist in any evaluation of the organization. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization use automated tools to collect data and otherwise support your organization's evaluation process? | HIPAA Reg Met | No | N/A | ORGANIZATION uses various tools to collect evidence to support an evaluation. For example, vulnerability scanning, pen testing, config management and log management. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization's evaluation process support the development of security recommendations? | HIPAA Reg Met | No | N/A | ORGANIZATION adds any challenge areas to the Risk Register where a POA&M is produced to ensure security recommendations are addressed depending on risk. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization documented each security evaluation finding, outlined mediation options and recommendations, and remediation decisions? | HIPAA Reg Met | No | N/A | ORGANIZATION adds any challenge areas to the Risk Register where a POA&M is produced to ensure security recommendations are addressed dependingon risk. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization documented the known security gaps after your security evaluation between the known risks and your mitigating security controls, and any acceptance of risk, including your organization's justification? | HIPAA Reg Met | No | N/A | ORGANIZATION adds any challenge areas to the Risk Register where a POA&M is produced to ensure security recommendations are addressed dependingon risk. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Has your organization developed a security program with established priorities and targets for continuous security improvement? | HIPAA Reg Met | No | N/A | ORGANIZATION has an established information security and privacy program with established priorities determined by the CSPC. In addition, Compliance brings any security improvements to the CSPC for consideration based on risk. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | In determining the best way to display evaluation results has your organization's written reports highlighted key findings and recommendations to be considered? | HIPAA Reg Met | No | N/A | ORGANIZATION adds any challenge areas identified by evaluation results to the Risk Register where a POA&M is produced to ensure security recommendations are addressed dependingon risk. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Does your organization circulate your final report to key staff, employees, and workforce members? | HIPAA Reg Met | No | N/A | Only ORGANIZATION RLT and the CSPC have purview to review final evaluation reports. |
| 164.308(a)(8) | 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 an entity's security policies and procedures meet the requirements of this subpart. | Evaluation is something that your organization does on its own either with internal resources or external expertise to make sure that your HIPAA Security controls are complete and fully protecting the ePHI that you maintain or create for your business. | Do you have a process, procedures in place to make sure that the document is available only to those designated to receive it? | HIPAA Reg Met | No | N/A | Only ORGANIZATION RLT and the CSPC have purview to review final evaluation reports. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization have business associate contracts? | HIPAA Reg Met | No | N/A | Any engagement dealing with ePHI has to have a signed BAA, per ORGANIZATION policy. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization's business associate agreements (as written and executed) contain sufficient language to ensure that required information types are protected? Including the 2009, 2010, and 2011 HITECH Act updates and inclusions? | HIPAA Reg Met | No | N/A | Applicable areas of HIPAA are addressed in ORGANIZATION's BAA template. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Has your organization identified the individual or department who is responsible for coordinating the execution of your organization's business associate agreements and other such agreements? | HIPAA Reg Met | No | N/A | ORGANIZATION has determined that the Compliance group, working with the external Legal department, have responsibility over handing and storing of BAA's. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization periodically review and reevaluate your list of business associates to determine who has access to ePHI in order to assess whether your list is complete and current? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures that all BAAs are reviewed annually per policy and standard. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Has your organization named your systems and functions covered by the contract/agreement? | HIPAA Reg Met | No | N/A | ORGANIZATION's system is known as a Decision Support System. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Are your organization's outsourced functions also covered by contracts/agreements? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures that all outsourced functions have contracts reviewed by Legal. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Are your organization's off-shore functions also covered by contracts/agreements? | HIPAA Reg N/A | N/A | N/A | ORGANIZATION does not have any off-shore functions. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Has your organization executed new and updated existing agreements or arrangements when necessary and appropriate? | HIPAA Reg Met | No | N/A | Applicable ORGANIZATION staff members have the responsibility to review contracts on an annual basis. Contracts are stored in a Google Drive folder. Most contracts don't change over time but if they do ORGANIZATION will make necessary updates to said contracts. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization's agreements and other arrangements include your business associate(s) roles and responsibilities for the ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION's organizational agreements include ORGANIZATION's business associate(s) roles and responsibilities for the ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization's agreements and other arrangements include security requirements that address confidentiality, integrity and availability of ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance has created an exhibit to be included in each contract covering security and privacy and the protection of ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do your organization's agreements and other arrangements include security requirements meet all the HIPAA Security Rule requirements per the HITECH Act? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance has created an exhibit to be included in each contract covering security and privacy and the protection of ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do your organization's agreements and other arrangements include the appropriate training requirements, as necessary? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance has created an exhibit to be included in each contract covering security and privacy and the protection of ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Who/which office within your organization is responsible for coordinating and preparing the final agreement(s) or arrangement(s)? | HIPAA Reg Met | No | N/A | ORGANIZATION has an outsourced Legal group that are responsible for coordinating and preparing the final agreement(s). |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do your organization's agreements and other arrangements specify how ePHI is to be transmitted to and from the business associate? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance has created an exhibit to be included in each contract covering security and privacy and the protection of ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do your organization's agreements and other arrangements specify necessary security controls? | HIPAA Reg Met | No | N/A | ORGANIZATION Compliance has created an exhibit to be included in each contract covering security and privacy and the protection of ePHI. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization conduct periodic security reviews on your business associates or covered entities? | HIPAA Reg Met | No | N/A | ORGANIZATION reviews BAAs on an annual basis, though most BAAs do not change over time depending on legislation. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Has your organization established criteria for measuring contract performance? | HIPAA Reg N/A | No | N/A | ORGANIZATION Customer Success established criteria for measuring contract performance |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do each of your organization's contracts or agreements include what service is being performed by the business associate? | HIPAA Reg Met | No | N/A | ORGANIZATION Customer Success ensures contracts or agreements include what service is being performed by the business associate |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Do each of your organization's contracts or agreements include expected outcome by the business associate? | HIPAA Reg Met | No | N/A | ORGANIZATION Customer Success ensures contracts or agreements include what service is being performed by the business associate |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization have in place a process for reporting security incidents related to the agreement? | HIPAA Reg Met | No | N/A | ORGANIZATION has a Compliance line for workforce members to report a concern. ORGANIZATION also has an email box for workforce members to report incidents. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization have in place a process to periodically evaluate the effectiveness of the business associate's security controls? | HIPAA Reg Met | No | N/A | ORGANIZATION has a vendor management program that evaluates security controls on vendors. In addition, ORGANIZATION uses a tool called Trackly to identify changes to Privacy Policies and Terms of Services for all vendors with notifications when any changes on their pages. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization have a process in place for terminating the contract, and has the business associate been advised what conditions would warrant termination? | HIPAA Reg Met | No | N/A | ORGANIZATION works with an external Legal group that has a process in place in the contracts for determining how contracts will be terminated. ORGANIZATION attempts to set contracts at one year at a time. |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | If your organization's business associate is a federal, state, or local government entity you may use a Memorandum of Understanding (MOU) to share ePHI. Does your MOU state all required safeguards for sharing ePHI? | HIPAA Reg N/A | N/A | N/A | N/A |
| 164.308(b)(1) | A covered entity, in accordance with164.306, 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. | Your organization has legal agreements called business associate agreements with your contractors and vendors who does work for your organization using or creating ePHI. | Does your organization know all the laws and regulations governing the use of ePHI by the governmental business associate? | HIPAA Reg Met | No | N/A | ORGANIZATION users a tool called Feedly to keep up with new laws and regulations governing the use of ePHI by the governmental business associate |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION have a formal access control policy that guided the development of access control procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a formal access control policy that guided the development of access control procedures |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has ORGANIZATION developed and implemented access control procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a formal access control policy and associated procedures. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Do ORGANIZATION's access control procedures include: 1) initial access, 2) increased access, 3) access to different systems and applications that user currently has? | HIPAA Reg Met | Partial | Medium | ORGANIZATION has an Access Control policy that covers initial access, change of access, and access to different systems. However, role changes are not adequately in place. Implement a control to document when changes to access change and the removal and addition of access. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has access control policy, including the rules of user behavior, been communicated to system users? | HIPAA Reg Met | No | N/A | ORGANIZATION ensures that all workforce members are notified when policies are changed. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has ORGANIZATION outlined how user compliance with access control policy will be enforced? | HIPAA Reg Met | No | N/A | ORGANIZATION has all workforce members sign the AUP, which is a summarization of applicable policies. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has ORGANIZATION determined who will manage the access control procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION's IT Team has overall ownership of Access Control. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION train users in access control procedures and management? | HIPAA Reg Met | No | N/A | ORGANIZATION's IT Team has overall ownership of Access Control and is trained in the procedure. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION train new employees/users in access control policy and procedures, and other instructions for protecting ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has all workforce members sign the AUP, which is a summarization of applicable policies. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION have procedures for new employee/user access to data and systems? | HIPAA Reg Met | No | N/A | During NEO, ORGANIZATION instructs the workforce how access will be granted to ePHI |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION have procedures for reviewing and, as appropriate, modifying access authorization for existing users? | HIPAA Reg Partially Met | Yes | High | ORGANIZATION may not have a comprehensive, repeatable process to evaluate/review all access.   ORGANIZATION should ensure that there is an access control review process. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has ORGANIZATION determined if the user identifier should be self-selected or randomly generated? Is it different for different types of data? | HIPAA Reg Met | No | N/A | ORGANIZATION issues unique user IDs to all employees. The employees have no choice on the matter. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Has ORGANIZATION determined if the user identifier should be self-selected or randomly generated? Is it different for different types of data? | HIPAA Reg Met | No | N/A | ORGANIZATION issues unique user IDs to all employees. The employees have no choice on the matter. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Can ORGANIZATION trace all system activity, viewing, modifying, deleting and creating of ePHI, to a specific user? | HIPAA Reg Partially Met | Partial | Medium | ORGANIZATION's needs and audit and log monitoring program that is in alignment with policy and standard. |
| 164.312(a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | You organization must assign each user a unique name or number within systems/organization. | Does ORGANIZATION record each time ePHI is viewed, modified, deleted or created in an audit tool to support audit and other business functions? | HIPAA Reg Partially Met | Partial | Medium | ORGANIZATION's needs and audit and log monitoring program that is in alignment with policy and standard. |
| 164.314(a)(1) | Business associate contracts or other arrangements. | This is the section that outlines the requirements for legal contracts, here called business associate agreements, and memorandum of understanding. | Does your organization have business associate agreements or other contracts with other health care entities? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(1)(i) | 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. | Business and legal documents | Does your organization's business associate agreements include mandated requirements? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(1)(ii) | A covered entity is not in compliance with the standards in 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful. | Business and legal documents | Do your organization's business associate agreements includes specified paragraphs on disclosures of business associates? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(1)(ii)(A) | Terminated the contract or arrangement, if feasible | Business and legal documents | Does your organization's business associate agreements includes specified paragraphs on termination of business associates? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(1)(ii)(B) | If termination is not feasible, reported the problem to the Secretary. | Business and legal documents | Does your organization's business associate agreements includes specified paragraphs if termination of business associates is not feasible, the issues is reported to the Office for Civil Rights? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(1)(ii)(B) | If termination is not feasible, reported the problem to the Secretary. | Business and legal documents | Does your organization include the following requirements and/or specifications, explicitly or by reference, in information acquisition contracts based on the assessment of risk and in accordance with applicable laws, regulations, and related guidance documents: security functional requirements/specifications? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)((ii) | Other arrangements. (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section | Business and legal documents | If your organization and the organization you are contract with are both governmental agencies do you use a memorandum of understanding (MOU)? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)((ii) | Other arrangements. (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section | Business and legal documents | Does your organization's MOU/agreement provide protection for the ePHI equivalent to those provided in at HIPAA business associate contract? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)((ii) | Other arrangements. (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) | Business and legal documents | If your organization's MOU cannot be terminated, are other enforcement mechanisms in place that are reasonable and appropriate? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)((ii)(1) | It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) | Business and legal documents | Does your organization use memorandum of understanding (MOU) with certain business associates? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)((ii)(2) | Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. | Business and legal documents | Does your organization have other laws similar to business associate agreement requirements that it must implement? | HIPAA Reg Met | No | N/A | ORGANIZATION has several state laws they are required to follow and are handled by MSA/contracts |
| 164.314(a)(2)((ii)(B) | If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. | Business and legal documents | If your organization has an MOU have you made a good faith effort to obtain satisfactory assurances that the HIPAA Security Standards are met? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(a)(2)((ii)(B) | If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. | Business and legal documents | Does your organization make the attempt to obtain satisfactory assurances, and the reasons that they cannot be obtained documented? | HIPAA Reg Met | No | N/A | ORGANIZATION has a vendor management procedure that ensures all documentation is collected. If not, ORGANIZATION works with the third party to gain assurance that their security/privacy program is adequate. |
| 164.314(a)(2)((ii)(C) | The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. | Business and legal documents | Does your organization or your contact partners have statutory obligations which requires the removal of the termination requirement? | HIPAA Reg Met | No | N/A | N/A |
| 164.314(a)(2)(i)(A) | Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity. | Business and legal documents | Does your organization's business associate contract(s) provide the business associates that will implement administrative, physical and technical safeguards to protect the ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(A) | Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity. | Business and legal documents | Does your organization's business associate contract(s) address functions related to creating, receiving, maintaining, and transmitting ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(A) | Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity. | Business and legal documents | Do your organization's business associate contracts provide that the business associates conduct a risk assessment that addresses administrative, physical and technical risks? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(B) | Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it. | Business and legal documents | Do your organization's business associate contracts provide that any agent, including a subcontractor, to whom the business associate provides ePHI, or access to such ePHI. agrees to implement reasonable and appropriate safeguards to protect the ePHI? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(C) | Report to the covered entity any security incident of which it becomes aware. | Business and legal documents | Does your organization's business associate contract(s) provide that the business associate will report any security incidents of which it becomes aware to the covered entity? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(C) | Report to the covered entity any security incident of which it becomes aware. | Business and legal documents | Has your organization identified the key business associate staff/point of contact in the event of a security incident? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(C) | Report to the covered entity any security incident of which it becomes aware. | Business and legal documents | Does your organization have in place a procedure including a reporting mechanism for reporting security incidents by a business associate? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(D) | Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. | Business and legal documents | Does your organizations business associate contract include standards and thresholds for termination of contract? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(D) | Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. | Business and legal documents | Do the conditions for termination within your organization's business associate contract include material breach of the contract, and that the breach cannot be cured? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(a)(2)(i)(D) | Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. | Business and legal documents | Does your organizations business associate contract include reporting the problem to Office for Civil Rights (OCR) if contract termination is not possible? | HIPAA Reg Met | No | N/A | ORGANIZATION has established BAAs with all other business associates and also ensures third parties have signed BAAs. |
| 164.314(b)(1) | Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to 164.504(f)(1)(ii) or (iii), or as authorized under 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | This area outlines the requirements for group health plans that share data with a plan sponsor for protection of the ePHI. | Is your organization a group health plan? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(1) | Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to 164.504(f)(1)(ii) or (iii), or as authorized under 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | This area outlines the requirements for group health plans that share data with a plan sponsor for protection of the ePHI. | Does your organization only share summary health information or disclose whether an individual is a participant or enrolled/unenrolled to the health plan sponsor? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Does your organization have group health plan documents that include plan sponsor requirements? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Does your organization amend your plan documents to incorporate provisions that require a health plan sponsor to implement administrative, physical and technical safeguards to protect the ePHI. Also, does the plan sponsor create, receive, maintain or transmit on your behalf? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Does your organization's plan document and ensure adequate separation between the group health plan and the plan sponsor, including sponsor's employees, classes of employees, or other persons who will be given access to the ePHI? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Do your organization's plan documents include provisions to require plan sponsor's agents, including subcontractors, to whom it provides ePHI agrees to implement all reasonable and appropriate security measures to protect the ePHI? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Do your organization's plan documents include provisions to require plan sponsor to report to the group health plan ay security incident of which it becomes aware? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Does your organization have a procedure in place that includes a mechanism for reporting security incidents by a plan sponsor? | HIPAA Reg N/A | No | N/A | N/A |
| 164.314(b)(2) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement safeguards. | Group health plans document requirements. | Does your organization have a procedure in place that includes a reporting mechanism for responding to security incidents by a plan sponsor? | HIPAA Reg N/A | No | N/A | N/A |
| 164.316(a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in subsection 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | A set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. | Does your organization have policies and procedures for administrative safeguards, physical safeguards, and technical safeguards? | HIPAA Reg Met | No | N/A | ORGANIZATION has policies and procedures for administrative safeguards, physical safeguards, and technical safeguards |
| 164.316(a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in subsection 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | A set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. | Does your organization have in place reasonable and appropriate polices and procedures that comply with the standards and implementation specifications of the HIPAA Security Rule? | HIPAA Reg Met | No | N/A | ORGANIZATION has in place reasonable and appropriate policies and procedures that comply with the standards and implementation specifications of the HIPAA Security Rule |
| 164.316(a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in subsection 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | A set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. | Does your organizations security policies and procedures take into consideration:  1) your organization's size, complexity and the services you provide.  2) your organization's technical infrastructure, hardware and software capabilities,  3) the cost of your organization's security measures,  4) the potential risks to day-to-day operation including which functions, and tools are critical to operations? | HIPAA Reg Met | No | N/A | ORGANIZATION has a set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. |
| 164.316(a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in subsection 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | A set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. | Does your organization have procedures for periodic revaluation of your security polices and procedures, and update them when necessary? | HIPAA Reg Met | No | N/A | ORGANIZATION has a set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. |
| 164.316(a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in subsection 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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | A set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. | Does your organization change security policies and procedures at any appropriate time, and document the changes and implementation? | HIPAA Reg Met | No | N/A | ORGANIZATION has a set of documents that describe an organization's policies for operation and the procedures necessary to fulfill the policies. |
| 164.316(b)(1) | Documentation. | Documentation is a multiplicity of documents in a chosen mix of media and with a certain collection to support your protection of PHI. | Does your organization have documente policy and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has developed and documented policies and standards for the Information security and privacy program. |
| 164.316(b)(1) | Documentation. | Documentation is a multiplicity of documents in a chosen mix of media and with a certain collection to support your protection of PHI. | Has your organization documented your decisions concerning the security management, operational, and technical controls to mitigate your identified risks? | HIPAA Reg Met | No | N/A | ORGANIZATION has documented decisions concerning the security management, operational, and technical controls to mitigate your identified risks through assessments and the Compliance Committee. |
| 164.316(b)(1) | Documentation. | Documentation is a multiplicity of documents in a chosen mix of media and with a certain collection to support your protection of PHI. | Does your organization update your security documentation following breaches, security incidents, new acquisitions, change in technology and other similar times? | HIPAA Reg Met | No | N/A | ORGANIZATION updates the security documentation following breaches, security incidents, new acquisitions, change in technology and other similar times, at least annually. |
| 164.316(b)(1) | Documentation. | Documentation is a multiplicity of documents in a chosen mix of media and with a certain collection to support your protection of PHI. | Does your organization have an individual or office that maintains and is responsible for your HIPAA Security documentation? | HIPAA Reg Met | No | N/A | ORGANIZATION has an individual or office that maintains and is responsible for your HIPAA Security documentation |
| 164.316(b)(1) | Documentation. | Documentation is a multiplicity of documents in a chosen mix of media and with a certain collection to support your protection of PHI. | Has your organization documented all security policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has organization documented all security policies and procedures |
| 164.316(b)(2) | Implementation specifications: | Documentation | Does your organization have a data retention policy and procedure(s) that consider all HIPAA retention requirements? | HIPAA Reg Met | No | N/A | ORGANIZATION has a data retention policy and procedure(s) that consider all HIPAA retention requirements |
| 164.316(b)(2)(i) | 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. | Documentation implementation specification | Has your organization aligned HIPAA documentation retention requirements with all other data retention polices? | HIPAA Reg Met | No | N/A | ORGANIZATION is aligned HIPAA documentation retention requirements with all other data retention polices |
| 164.316(b)(2)(ii) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | Documentation implementation specification | Has your organization communicated with all staff that need access to your security documentation where it is found? | HIPAA Reg Met | No | N/A | ORGANIZATION has communicated with all staff that need access to your security documentation where it is found |
| 164.316(b)(2)(ii) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | Documentation implementation specification | Does your organization's education, training and awareness activities include the availability of your security documentation? | HIPAA Reg Met | No | N/A | ORGANIZATION’s education, training and awareness activities include the availability of your security documentation |
| 164.316(b)(2)(ii) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | Documentation implementation specification | Does your organization have a process in place to solicit input from the staff, employees, and workforce impacted, into your updates of your security policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has a process in place to solicit input from the staff, employees, and workforce impacted, into your updates of your security policies and procedures |
| 164.316(b)(2)(iii) | Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. | Documentation implementation specification | Does your organization have a version control for your procedure(s) and process for the verification of the timeliness of your security policies and procedures? | HIPAA Reg Met | No | N/A | ORGANIZATION has version control for procedure(s) and process for the verification of the timeliness of your security policies and procedures |
| 164.316(b)(2)(iii) | Standard: Contingency plan. 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. | Your organization must have policies and procedures to respond to an unforeseen event, and unpredictable event; in other words to an event that may or may not happen. | Has your organization defined your overall contingency objectives? Does it include a listing of all areas that use ePHI? | HIPAA Reg Not Met | Yes | High | We have not seen the contingency plan |