assessIT.io

Sample Health System

Shawn Helwig

HIPAA Security Rule 2.0 Readiness Assessment Results

09/23/2025

Table of Contents

Contents

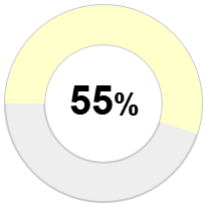
Summary: Overall Results

This comprehensive evaluation tool has been built to help Covered Entities and Business Associates prepare for the significant updates proposed in the 2024 revision of the HIPAA Security Rule. Developed by seasoned healthcare cybersecurity consultants, this assessment considers key administrative, technical, and physical safeguard requirements—integrating the newly proposed requirements for vulnerability scanning, penetration testing, system patching timelines, enhanced policy documentation, and more—to help you determine how well prepared your organization is for the HIPAA Security Rule 2.0.

The assessment considers your organization's readiness across 13 security domains aligned to the currently proposed HIPAA 2.0 Security Rule. Your overall readiness score is shown below, along with individual readiness scores and ratings for each of the security domains. Additionally, the assessment considers a number of critical safeguards that are especially important in achieving ultimate compliance. These results will help you target key weaknesses where improvements are required.

There is a link and the end of these results to download a summary report highlighting areas of compliance strength and risk exposure, as well as prioritized recommendations for remediation and policy refinement. The report will also be emailed to you shortly.

Your Overall Readiness Score is:



Your Readiness Rating is:

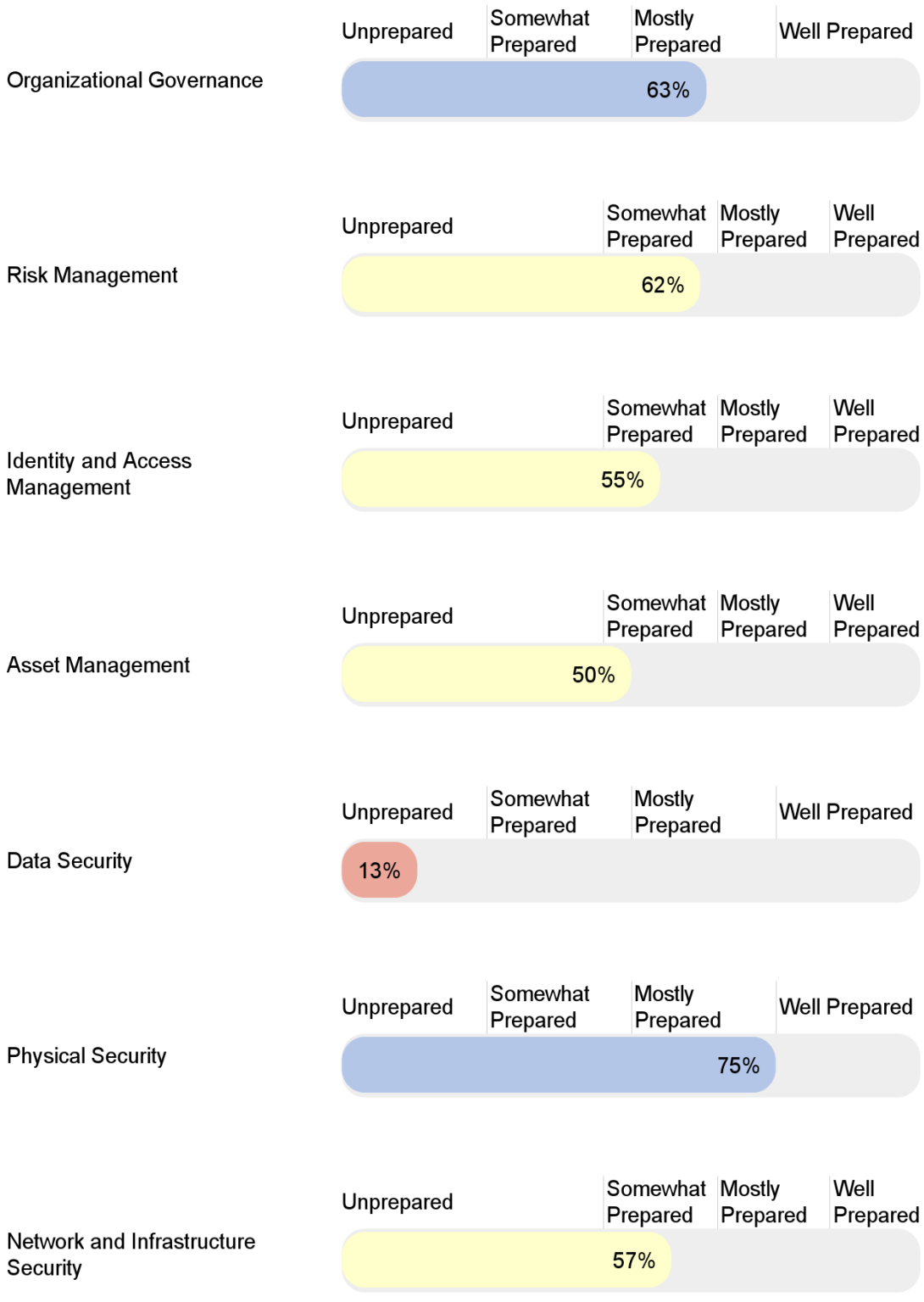
Somewhat Prepared

Overall Readiness Assessment Findings:

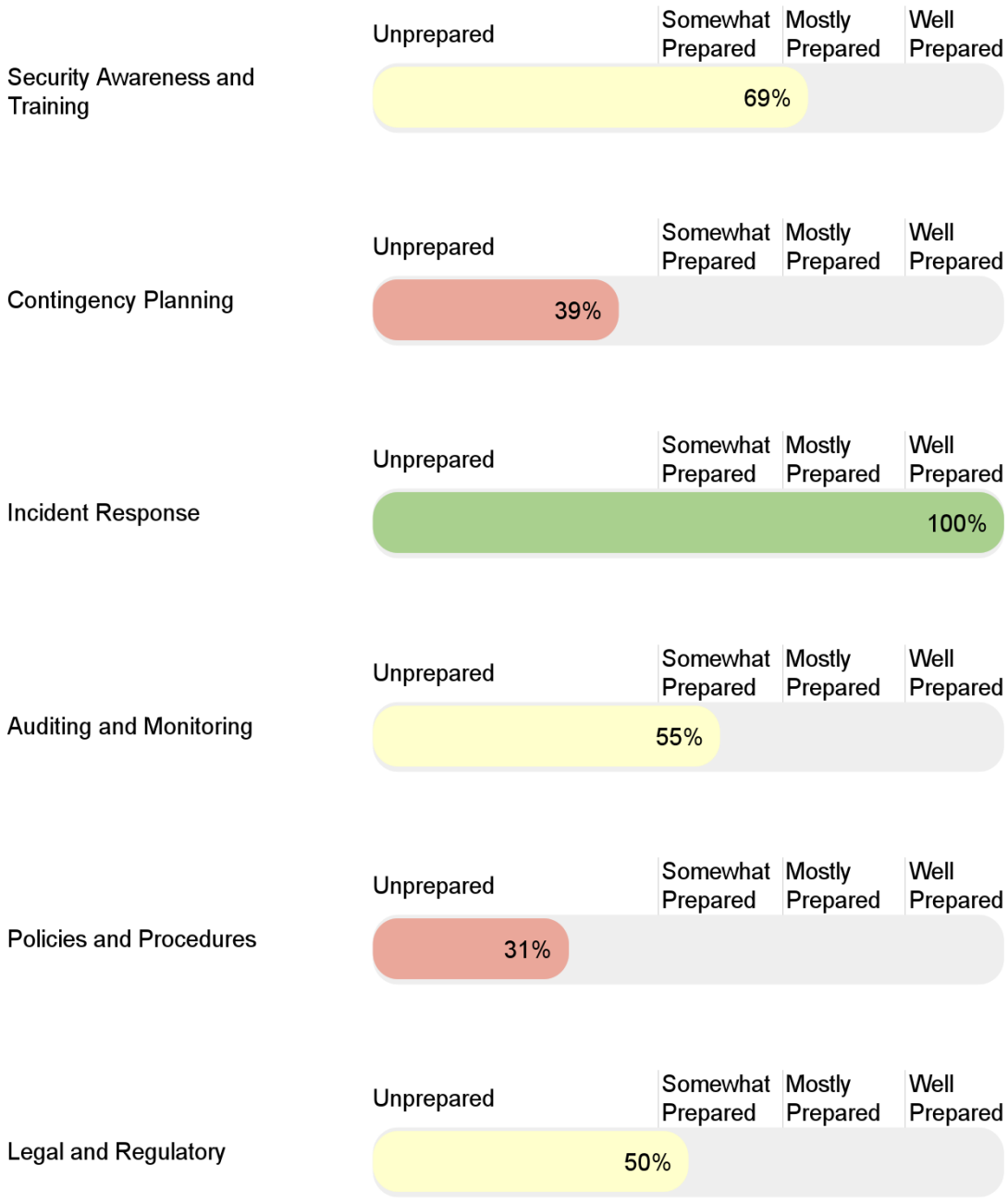
Basic security policies and procedures exist but are inconsistently applied. The organization has started to recognize the importance of structured security practices, but implementation varies. Compliance efforts are often project-driven, not integrated into a broader program.

* Initial documentation of controls and processes
* Partial alignment with security frameworks or standards
* Some roles and responsibilities are defined
* Security awareness and training are emerging

Readiness Scores by Security Domain:



Readiness Scores by Security Domain (cont.):



Legend

In the next section, you will receive feedback on each of the thirteen Security Domains represented by this assessment. Each Security Domain will have a brief definition followed by a graphic that depicts your score in that Security Domain. Below the scoring graphic, you will find each of the subsections as defined below:

Assessment Findings: Aggregated results by security domain identified during the assessment process.

Critical Safeguards: Essential security controls or measures that provide the highest level of protection against significant risks or threats.

Key Weaknesses: Notable gaps or deficiencies in controls, processes, or systems that could expose the organization to risk if not addressed.

Given that the size and scope of the question pool for each Security Domain varies, the *Organizational Governance* and *Physical Security* Domains do **NOT** have a Critical Safeguards or Key Weaknesses section. Additionally, the *Identity and Access Management* and *Network and Infrastructure Security* Domains each have **two** possible Critical Safeguards and Key Weaknesses.

Finally, the Overall Readiness Score is calculated based on ALL of the questions in the assessment being of equal value.

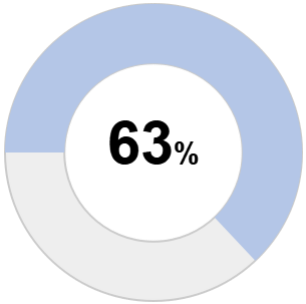
Disclaimer

This assessment is based on the 2024 *Proposed* Changes to the HIPAA Security Rule as published by the U.S. Department of Health and Human Services (HHS). The final rule, once issued, may differ in part or in whole from the proposed version. Some provisions may be adopted without change, others may undergo revisions that affect their scope or implementation requirements, and certain proposed provisions may not be included in the final rule. Organizations should be aware that this assessment reflects the state of the proposed rule at the time of preparation and should not be interpreted as a definitive statement of future regulatory obligations. For authoritative requirements, organizations must refer to the final rule as published in the Federal Register and official HHS guidance.

Security Domain: Organizational Governance

Organizational policies, roles, and oversight structures are established and maintained to ensure that cybersecurity responsibilities and decisions align with the organization's mission, legal and regulatory requirements, and risk tolerance.

Your Organizational Governance Score is:



Your Rating is: Mostly Prepared

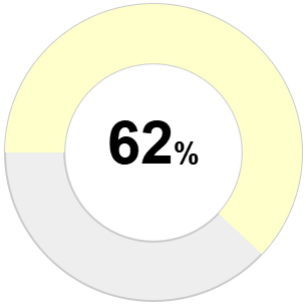
Assessment Findings:

Governance structures are formally established, documented, and consistently applied across the organization.

Security Domain: Risk Management

Cybersecurity risks to organizational operations, assets, and individuals are identified, assessed, prioritized, and managed as part of an enterprise risk management strategy that supports informed decision-making and resource allocation.

Your Risk Management Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Risks are being identified and assessed, but prioritization and tracking are inconsistent.

Critical Safeguards:

In your organization, Risk Management is **not a Key Weakness!**

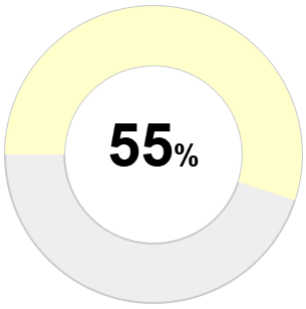
Key Weakness Findings:

Your organization has no key weakness in Risk Management.

Security Domain: Identity and Access Management

Access to organizational resources is managed through the identification and authentication of users, devices, and systems, ensuring that only authorized entities are granted access based on business needs and least privilege principles.

Your Identity and Access Management Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Some access controls are in place; limited use of least privilege or role-based access.

Critical Safeguards:

- Revoking employee access to ePHI is **not a Key Weakness!**
- Multi-factor identification is **a Key Weakness!**

Key Weakness Findings:

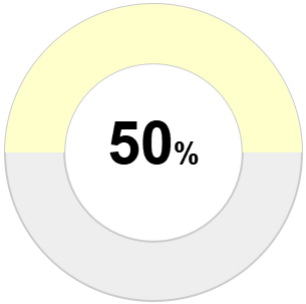
Your organization has no key weakness in revoking employee access to ePHI.

The failure to implement multifactor authentication for ePHI systems increases risk in healthcare by leaving sensitive patient health information vulnerable to breaches through stolen or weak credentials, potentially resulting in identity theft, medical fraud, regulatory violations, and disrupted patient care.

Security Domain: Asset Management

Assets that support business functions—including data, hardware, software, systems, and services—are inventoried and managed based on their criticality to organizational operations and in alignment with the organization's cybersecurity risk strategy.

Your Asset Management Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Basic asset inventory is maintained for key systems, but lacks categorization or prioritization.

Critical Safeguards:

In your organization, Asset Management is **not a Key Weakness!**

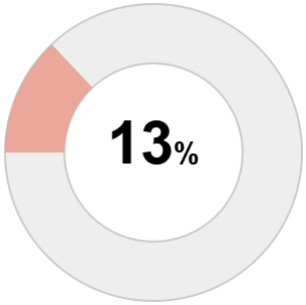
Key Weakness Findings:

Your organization has no key weakness in Asset Management.

Security Domain: Data Security

Data is managed and protected throughout its lifecycle to ensure its confidentiality, integrity, and availability, consistent with its sensitivity, criticality, and the organization's risk management policies.

Your Data Security Score is:



Your Rating is: Unprepared

Assessment Findings:

Data protection is informal or ad hoc; no classification or encryption strategy.

Critical Safeguards:

In your organization, Data Security is **a Key Weakness!**

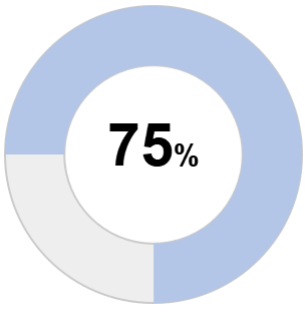
Key Weakness Findings:

Inadequate protection of sensitive data—whether at rest, in transit, or in use—compromises confidentiality, integrity, and availability. A lack of encryption in this area reveals a systemic failure to meet HIPAA's foundational safeguard requirements for ePHI.

Security Domain: Physical Security

Physical access to systems, devices, and facilities is restricted and monitored to prevent unauthorized access, damage, or interference with organizational resources.

Your Physical Security Score is:



Your Rating is: Mostly Prepared

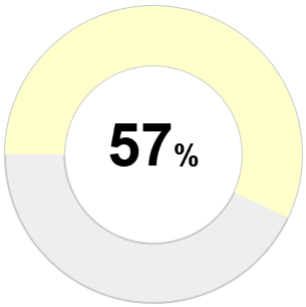
Assessment Findings:

Access controls, monitoring, and surveillance are consistently enforced across all sensitive areas.

Security Domain: Network and Infrastructure Security

Network infrastructure and communications are secured through the use of segmentation, access controls, and monitoring to protect against unauthorized access and ensure data integrity and confidentiality.

Your Network and Infrastructure Security Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Firewalls and basic segmentation are in place. Monitoring is limited.

Critical Safeguards:

- Patch/Update Management is **not a Key Weakness!**
- Maintaining secure baseline configurations is **a Key Weakness!**

Key Weakness Findings:

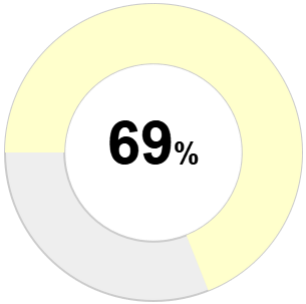
Your organization does not have a key weakness in patch/update management.

A failure to implement and maintain effective patch management and secure baseline configurations for software and operating systems exposes healthcare organizations to heightened risks of cyber-attacks, such as ransomware and malware exploitation, leading to massive data breaches of protected health information, operational disruptions that delay critical patient care.

Security Domain: Security Awareness and Training

A regulated entity would be required to provide role-based security awareness training to a new workforce member within a reasonable period of time, but no later than 30 days after the workforce member first has access to the regulated entity's relevant electronic information systems.

Your Security Awareness and Training Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Security training is delivered periodically but is not role-based or tracked.

Critical Safeguards:

In your organization, Security Awareness and Training is **not a Key Weakness**

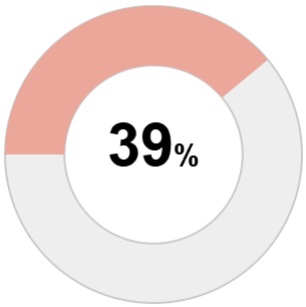
Key Weakness Findings:

Your organization does not have a key weakness in Security Awareness and Training.

Security Domain: Contingency Planning

Plans and procedures are established, maintained, and tested to ensure the organization can continue essential operations and recover from cybersecurity events, disasters, or other disruptions.

Your Contingency Planning Score is:



Your Rating is: Unprepared

Assessment Findings:

No formal plans exist for disaster recovery or business continuity.

Critical Safeguards:

In your organization, Contingency Planning is **not a Key Weakness!**

Key Weakness Findings:

Your organization does not have a key weakness in Contingency Planning.

Security Domain: Incident Response

Processes are in place to detect, respond to, contain, and recover from cybersecurity incidents in a timely and coordinated manner to minimize impact and support business continuity.

Your Incident Response Score is:

Your Rating is: Well Prepared

Assessment Findings:

Response is integrated with monitoring, threat intelligence, and lessons learned are used for continuous improvement.

Critical Safeguards:

In your organization, Incident Response is **not a Key Weakness!**

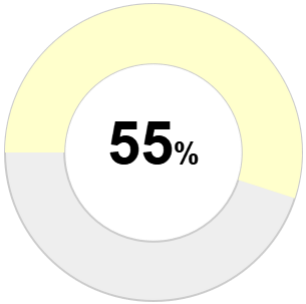
Key Weakness Findings:

Your organization does not have a key weakness in Incident Response.

Security Domain: Auditing and Monitoring

Security-relevant activities and system behaviours are continuously logged, reviewed, and analysed to detect anomalous events, support investigations, ensure policy compliance, and enable timely response to potential threats in alignment with organizational risk tolerance and regulatory obligations.

Your Auditing and Monitoring Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Key logs are reviewed periodically, but there is limited correlation or alerting.

Critical Safeguards:

In your organization, Auditing and Monitoring is **not a Key Weakness!**

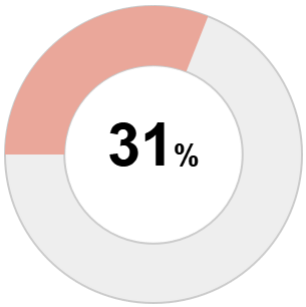
Key Weakness Findings:

Your organization does not have a key weakness in Auditing and Monitoring.

Security Domain: Policies and Procedures

Documented policies and standard operating procedures are developed, communicated, and enforced to guide the consistent implementation of cybersecurity practices across the organization.

Your Policies and Procedures Score is:



Your Rating is: Unprepared

Assessment Findings:

Few or no documented policies exist; practices vary by individual/team.

Critical Safeguards:

In your organization, Policies and Procedures is **not a Key Weakness!**

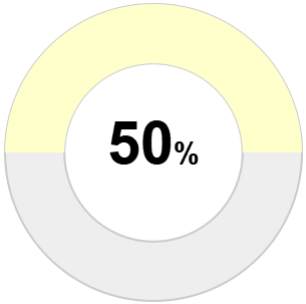
Key Weakness Findings:

Your organization does not have a key weakness in Policies and Procedures.

Security Domain: Legal and Regulatory

Legal, statutory, regulatory, and contractual cybersecurity requirements applicable to the organization are identified, understood, and incorporated into policies, processes, and controls to ensure ongoing compliance and to reduce the risk of legal exposure or enforcement actions.

Your Legal and Regulatory Score is:



Your Rating is: Somewhat Prepared

Assessment Findings:

Some regulatory requirements are identified and addressed in basic policies.

Critical Safeguards:

In your organization, Legal and Regulatory is **a Key Weakness!**

Key Weakness Findings:

Failure to require Business Associates to annually verify the implementation of technical safeguards, as required under the HIPAA Security Rule, indicates a significant oversight in third-party risk management. This lack of due diligence exposes the organization to regulatory noncompliance and elevates the risk of ePHI compromise through inadequately secured partner systems. HIPAA places accountability on covered entities to ensure that all parties handling ePHI uphold the same security standards, and a negative response to this control reflects a systemic breakdown in fulfilling that responsibility.

Next Steps

Thank you for taking the HIPAA Security Rule 2.0 Readiness Assessment.

We encourage you to review the findings carefully with your compliance and security leadership teams. As the regulatory landscape continues to evolve, early awareness and strategic planning are essential.

If required, the following electronic signature indicates that the signer has completed this assessment truthfully and to the best of their ability.

Name:	Title:
Shawn Helwig	CEO

If you have HIPAA-specific questions or need professional assistance to prepare for the new HIPAA regulations, please use this link to submit a request for expert help:

Click Here

assessIT.io will connect you with a HIPAA professional who will talk through your situation. If you do not request contact from an expert, we **NEVER** share your information. We **WILL** follow up with you on occasion to see if you think it is time to complete the readiness assessment again to track your progress. Let us know if you would like to take the assessment again, and we will send you a discount code to save $250.

Finally, please let us know if you have any feedback for us. Thank you!

The **assessIT.io** Team
info@assessit.com

Appendix – Questions & Responses

All the assessment questions and your responses are shown in the tables below. For each question where your score is less than 4, there is an opportunity to improve your practices to be better prepared for the HIPAA 2.0 regulations.

Organizational Governance

Question	Response	Score
1) [redacted]	Yes, the organization has established compensating controls for reasonable exceptions to standard policies, and these controls are reviewed annually to ensure they are effective and compliant.	4 out of 4
2) [redacted]	No, we have not classified any specifications as "addressable," or we have not handled them appropriately. All specifications are either treated as "required" or not documented.	1 out of 4
Notes:		

Risk Management

Question	Response	Score
3) [redacted]	Within 12 Months	3 out of 4
4) [redacted]	A documented risk analysis exists but is outdated or lacks sufficient detail to fully assess threats and vulnerabilities.	2 out of 4
5) [redacted]	The risk analysis is comprehensive and includes a complete, dynamic inventory of all technology assets, including cloud services, mobile devices, and medical equipment, with clear linkage to where ePHI is stored or transmitted.	4 out of 4
6) [redacted]	The risk analysis includes a current, detailed, and actively maintained network map that supports the identification of risks to ePHI across all internal and external	4 out of 4

	connections, including VPNs, cloud services, and third-party integrations.	
7) [redacted]	Yes, we conduct and document a risk analysis every year that includes some key threats to ePHI, but we do not have a structured process to identify all reasonably anticipated threats.	2 out of 4
8) [redacted]	No, our risk analysis does not currently address vulnerabilities or predisposing conditions related to our ePHI systems.	0 out of 4
9) [redacted]	Yes, our risk analysis includes a thorough assessment and documentation of all security measures in place to protect ePHI, and we review and update this documentation regularly.	4 out of 4
10) [redacted]	Yes, our risk analysis thoroughly evaluates and documents the likelihood of each identified threat exploiting vulnerabilities, using a structured methodology to assess and prioritize risks.	4 out of 4
11) [redacted]	Our risk analysis considers the potential impact of threats, but it is based on general assumptions and does not always document the specific impact of each threat.	2 out of 4
12) [redacted]	Yes, we assess the risk level for each threat and vulnerability, but the process may lack consistency or detailed documentation for some threats and vulnerabilities.	3 out of 4
13) [redacted]	Yes, we assess risks to ePHI when entering into or renewing business associate agreements, but the written verification from business associates is not always consistently reviewed or documented.	3 out of 4
14) [redacted]	The organization has a written Risk Management Plan that is reviewed at least every 24 months.	2 out of 4
15) [redacted]	Yes, we have a documented schedule for testing the effectiveness of security controls at least once per year, and we consistently	4 out of 4

[redacted] effectiveness of security controls at least once per year?	adhere to this schedule with comprehensive testing procedures.	
16) [redacted] How does your organization validate that security measures remain effective against evolving threats?	We occasionally review and update our security measures based on evolving threats, but we do not have a formal or regular process for validating their effectiveness.	2 out of 4
17) [redacted] Who is accountable for conducting and documenting these evaluations of security measures?	We do not perform annual reviews	0 out of 4
Notes:		

Identity and Access Management

Question	Response	Score
18) [redacted] Does your organization have a documented process for promptly revoking employee access to ePHI within an hour of termination?	Yes, we have a formal process that ensures all workforce member access to systems and ePHI is terminated within one hour of their employment or arrangement ending, and this is consistently followed.	4 out of 4
19) [redacted] Are access revocation timelines tracked and monitored to ensure compliance with the 24-hour requirement?	No, we do not track or monitor access revocation timelines, and we do not have a formal process to ensure compliance with the 24-hour requirement.	0 out of 4
20) [redacted] How does your organization handle emergency access removal in security incidents?	We have an established process for emergency access removal during security incidents, but there may be occasional delays in execution due to manual intervention or lack of automation.	3 out of 4
21) [redacted] Have you implemented multi-factor authentication (MFA) for access to ePHI, and are they enforced across all systems handling ePHI?	MFA has been implemented on a limited basis for systems handling ePHI, but enforcement is not mandatory, and not all users are required to use it.	1 out of 4
22) [redacted] If there are exceptions to the use of MFA, how are they justified and documented?	Exceptions to the use of MFA are documented with justifications, and they are approved by management, but reviews are not performed regularly or consistently.	3 out of 4
Notes:		

Asset Management

Question	Response	Score

23) [redacted]	A comprehensive and actively maintained asset inventory is in place, covering all hardware and software assets (including cloud and mobile devices), with linkage to ownership, ePHI data flows, and risk management processes.	4 out of 4
24) [redacted]	Never	0 out of 4
25) [redacted]	The inventory includes all known hardware assets that store, transmit, or process ePHI and is reviewed periodically.	3 out of 4
26) [redacted]	Most software systems are inventoried, but updates are infrequent or certain categories (e.g., cloud apps, mobile apps, or utilities) are excluded.	2 out of 4
27) [redacted]	Most business-critical cloud services are inventoried, but some SaaS tools or shadow IT may be missing or undocumented.	2 out of 4
28) [redacted]	Only major databases are acknowledged, with limited or no documentation of the type or location of ePHI.	1 out of 4
29) [redacted]	A network map is in place for core infrastructure but may not include endpoints, wireless, remote access, or cloud interconnections.	2 out of 4
30) [redacted]	Yes, we have an inventory of technology assets handling ePHI, but updates are only done on an ad-hoc basis.	2 out of 4
31) [redacted]	All assets that store, transmit, or process ePHI are uniquely identified using standardized naming or tagging conventions and recorded in the inventory.	3 out of 4
32) [redacted]	ePHI systems have minimal controls to disable or suspend access after unsuccessful login attempts, and the enforcement of these controls is inconsistent or not regularly reviewed.	1 out of 4
Notes:		

Data Security

Question	Response	Score
33) [redacted]	No, we have not implemented network segmentation to protect ePHI, and there are no plans to do so.	0 out of 4
34) [redacted]	ePHI data is encrypted at rest but not in transit or it is encrypted in transit but not at rest.	1 out of 4
Notes:		

Physical Security

Question	Response	Score
35) [redacted]	Yes, physical safeguards are in place for most workstations with access to ePHI, but some areas may not be fully covered or reviewed consistently.	3 out of 4
Notes:		

Network and Infrastructure Security

Question	Response	Score
36) [redacted]	We have a patching process in place, but our timelines for addressing critical risks within 15 calendar days are not always met, and we may not consistently use the results from all the required assessments to guide the process.	2 out of 4
37) [redacted]	We update our network map annually and in response to changes in regulatory environment, to reflect all changes in ePHI flow.	3 out of 4
38) [redacted]	We update the asset inventory and network map only after major operational or environmental changes, and updates are performed on an ad-hoc basis without a formal process.	2 out of 4
39) [redacted]	Yes, we deploy anti-virus and anti-malware controls on most technology assets, but some systems may not be fully covered or regularly updated.	3 out of 4

40) [redacted]	Yes, we have a process to identify and remove extraneous software, but it is not consistently applied or regularly reviewed. Updates are done on an ad-hoc basis when issues are identified.	3 out of 4
41) [redacted]	We attempt to configure and secure operating systems and software in alignment with our risk analysis, but the process is informal and not regularly reviewed or updated.	1 out of 4
42) [redacted]	We disable network ports and unnecessary software for some systems based on the risk analysis, but the process is not consistently applied to all systems across the organization.	2 out of 4
43) [redacted]	We conduct vulnerability scans every 6 months, but some vulnerabilities identified in the scans have not been fully addressed or mitigated yet.	3 out of 4
44) [redacted]	The last vulnerability scan identified several vulnerabilities, but only high-severity issues were addressed. Lower-severity vulnerabilities have not yet been prioritized or remediated.	2 out of 4
45) [redacted]	Vulnerabilities are identified sporadically using automated tools, but remediation is not always based on severity, and some vulnerabilities may remain unresolved for extended periods.	2 out of 4
46) [redacted]	We monitor authoritative sources occasionally, but not consistently. Our monitoring may be limited to major security advisories or incidents, and we do not always follow up on all identified threats or vulnerabilities.	2 out of 4
47) [redacted]	In addition to vendor sources, we receive alerts and newsletters from various industry sources that share relevant threat information.	2 out of 4
48) [redacted]	We perform penetration testing infrequently, not on a regular 12-month cycle, and some systems are not tested at all.	1 out of 4
49) [redacted]	We use automated tools to identify vulnerabilities regularly, and a process is in place for remediation, but the prioritization and remediation may not always be timely or consistent.	3 out of 4

50) [redacted]	Some systems and devices still use default passwords, and there is no formal process in place to ensure they are changed to strong, unique passwords.	3 out of 4
Notes:		

Security Awareness and Training

Question	Response	Score
51) [redacted]	All new workforce members receive role-based security awareness training within 30 days, tailored to their job functions and access to ePHI, tracked for compliance, and integrated with other onboarding workflows such as access provisioning and policy attestation.	4 out of 4
52) [redacted]	Most workforce members complete annual security awareness training, but the process is not enforced or role-specific.	2 out of 4
53) [redacted]	The organization publishes annual security reminders or threat alerts.	2 out of 4
54) [redacted]	New hire and annual security awareness training is tracked and security awareness reminders are tracked in a spreadsheet or similar document.	3 out of 4
Notes:		

Contingency Planning

Question	Response	Score
55) [redacted]	Yes, we have conducted a criticality analysis, and restoration priorities are generally defined. However, the analysis is not regularly reviewed or updated.	3 out of 4
56) [redacted]	We have established procedures for restoring critical systems and data, but the 72-hour restoration timeline is not consistently met or documented in all cases.	2 out of 4
57) [redacted]	Backups for critical ePHI systems run sporadically, with no set schedule for every 48 hours. Some systems may not	1 out of 4

	be fully covered by backups, and the testing of backups is rarely performed.	
58) [redacted]	Backup failures and errors are not notified in real-time. There may be a manual process for checking failures, but notifications and corrective actions are often delayed.	1 out of 4
59) [redacted]	The backup solution generates log files that record the success and failure of backups, but error conditions are not consistently logged or reviewed.	2 out of 4
60) [redacted]	We have not performed an exercise or test of the data backups.	0 out of 4
61) [redacted]	There is a process in place for notifying the group health plan, but notifications may not always occur within the required 24-hour timeframe, and reviews of the process are infrequent.	2 out of 4
Notes:		

Incident Response

Question	Response	Score
62) [redacted]	Yes, we have a comprehensive, written Security Incident Response Plan (SIRP) that clearly defines the process for reporting and responding to security incidents. The plan is regularly reviewed, tested, and updated to ensure effectiveness.	4 out of 4
63) [redacted]	Quarterly	4 out of 4
64) [redacted]	Monthly	4 out of 4
65) [redacted]	Yes, we maintain comprehensive and detailed documentation of all security incidents, including timelines, responses, lessons learned, and outcomes. This documentation is regularly reviewed and used to improve our security posture.	4 out of 4
Notes:		

Auditing and Monitoring

Question	Response	Score
66) [redacted]	We have a written policy and procedures for the ISAR process, but the review process is not formal, and the policy is reviewed infrequently, usually only when issues arise.	2 out of 4
67) [redacted]	Audit trails are included for some systems, but coverage is incomplete or the review process lacks defined frequency and criteria.	2 out of 4
68) [redacted]	Event logs for systems that store, transmit, or process ePHI are consistently included in the ISAR process and reviewed at defined intervals.	3 out of 4
69) [redacted]	Firewall logs are reviewed during investigations or specific incidents but are not consistently analyzed as part of routine ISAR processes.	2 out of 4
70) [redacted]	System logs are reviewed for select applications or servers but coverage is incomplete and lacks regular review cycles.	2 out of 4
71) [redacted]	Backup logs are generated but rarely reviewed or tied to ISAR activities.	1 out of 4
72) [redacted]	User access reports are centrally collected and routinely reviewed as part of a formal ISAR process, with automated alerts for anomalous behavior, role-based access pattern analysis, and integration with identity and access management, incident response, and audit readiness workflows.	4 out of 4
73) [redacted]	Logs from anti-malware software are reviewed for select systems or after specific incidents, but reviews are not part of a routine ISAR process.	2 out of 4
74) [redacted]	Security incidents are sometimes documented, but reports are informal and not consistently reviewed.	1 out of 4
75) [redacted]	Monthly	3 out of 4
76) [redacted]	Less than 1 Month or Limited to Disk Capacity	0 out of 4
77) [redacted]	We will record it as an incident but take no further action.	1 out of 4

[redacted]		
78) [redacted]	Yes, the ISAR procedures are reviewed and tested every 12 months, but some updates may be delayed or may not fully address all potential security risks.	3 out of 4
79) [redacted]	A HIPAA audit was performed at some point in the past, but it is not conducted regularly or formally documented.	1 out of 4
80) [redacted]	Yes, real-time activity is logged in all electronic systems, and logs are regularly monitored, analyzed, and retained according to policy to ensure compliance with security and audit requirements.	4 out of 4
81) [redacted]	Yes, the Security Official reviews and documents the implementation and effectiveness of compensating controls during their use, and this process is conducted regularly to ensure that the controls remain effective in securing ePHI and relevant systems.	4 out of 4
Notes:		

Policies and Procedures

Question	Response	Score
82) [redacted]	We have a written sanction policy, but it is reviewed infrequently, typically only when issues arise, and may not be formally updated every 12 months.	2 out of 4
83) [redacted]	We have written policies, procedures, and security plans that meet most HIPAA requirements, but some areas may not be fully covered or require updates for full compliance.	2 out of 4
84) [redacted]	Policy and procedure review frequency occurs when an event triggers it.	1 out of 4
85) [redacted]	No, group health plan sponsors do not have documented policies for implementing HIPAA security safeguards, and there is no plan to develop them.	0 out of 4
Notes:		

Legal and Regulatory

Question	Response	Score
86) [redacted]	No, we do not require our business associates to verify their technical safeguards, and there is no process in place to ensure compliance with this requirement.	0 out of 4
87) [redacted]	Yes, we have formal, documented procedures in place for notifying covered entities or business associates immediately when a contingency plan is activated. These procedures are regularly reviewed and tested for effectiveness.	4 out of 4
88) [redacted]	Most agents handling ePHI have agreed to comply with HIPAA safeguards, but some may not have signed formal agreements, and the agreements are not always reviewed or updated.	2 out of 4
Notes:		