

HIPAA RISK ASSESSMENT

2/21/2020



ABC COMPANY TECHNICAL REPORT

*Technical report of HIPAA Risk Assessment
performed for ABC Company.*

HIPAA RISK ASSESSMENT

ABC Company

Overview

Ascend Technologies was contracted by ABC Company to perform a HIPAA Risk Assessment focused on HIPAA HITECH. The goal of a HIPAA Risk Assessment is determining the status of an organization's information security posture and highlight gaps that may expose the organization to unnecessary risk as well as to identify gaps in compliance to HIPAA HITECH. This document provides an overview of the findings from the assessment and recommendations for addressing risks identified through the assessment process.

Approach

Ascend Technologies' risk assessment approach is what separates us from our competition. There are many firms that can perform automated penetration testing and generate a report – or go through a checklist to determine “compliance with best practices”. Ascend Technologies' approach provides increased business value in the following ways:

- Our findings are custom written for your organization. Anyone can run some automated tools and identify vulnerabilities, but our strength lies in being able to manually verify those detected issues and then communicate them in terms of potential business impact along with sensible recommendations for correcting the discovered security weaknesses. In other words, we'll help you to understand what each particular risk really means to your organization and exactly how someone could go about exploiting that vulnerability.
- We educate our client throughout the process. In our view, it would be a great disservice to do an assessment, deliver a report with findings and recommendations and then walk away. We prefer to work as partners with our clients, helping them to understand the many information security challenges and compliance requirements being faced and to develop an appropriate and cost-effective approach for dealing with those challenges.
- Our extensive work in harmonizing standards and best practices and then integrating them into our assessment method ensures that your organization is prepared to meet not just today's information security requirements, but tomorrow's as well.
- Ascend Technologies' approach is consultative and educational. We will help you identify which information security requirements and guidelines may apply to your organization. We can translate these lengthy texts into plain English, in terms of what it means to your business and what, if anything needs to be done.

Contents

HIPAA RISK ASSESSMENT	1
.....	2
Overview.....	2
Approach	2
HIPAA Compliance Methodology.....	3
HIPAA Assessment and Results	3
HIPAA Administrative Safeguards.....	3
Security Management Process 164.308(a)(1).....	3
Assigned Security Responsibility 164.309(a)(2) (Required)	3
Security Management Process 164.308(a)(3).....	3
Information Access Management 164.308(a)(4)	3
Security Awareness and Training 164.308(a)(5).....	3
Security Incident Procedures 164.308(a)(6)	3
Contingency Plan 164.308(a)(7)	3
Evaluation 164.308(a)(8).....	3
Business Associate Contracts and Other Arrangements 164.308(b)(1).....	3
Physical Safeguards.....	3
Facility Access Controls 164.310(a)(1)	3
Workstation Use 164.310(b)	3
Workstation Security 164.310(c).....	3
Device and Media Control 164.310(d)(1)	3
Technical Safeguards.....	3
Access Control 164.312(a)(1)	3
Audit Control 164.312(b)	3
Integrity 164.312(c)(1)	3
Person or Entity Authentication 164.312(d)	3
Transmission Security 164.312(e)(1)	3
Critical Controls Overall Score.....	3
Vulnerability Assessment	3
Summary of Results	3
Recommendations.....	3
Conclusions.....	3

HIPAA Compliance Methodology

Ascend Technologies has developed an assessment methodology based upon the HIPAA Security Rule (45 C.F.R. §§ 164.302 – 318). The HIPAA Security Rule is a national standard to protect individual's electronic personal health information (e-PHI) that is created, received, used or maintained by a HIPAA covered entity. The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions of the rule. Ascend Technologies used this guidance as well as past experience and training to develop this assessment and produce this report.

HIPAA Assessment and Results

Ascend Technologies has taken the HIPAA Security Rule and integrated it with our HIPAA Risk Assessment methodology. There are a total of 42 standards and implementation specifications associated with the HIPAA Security Rule. These standards and implementation specifications are either "required" or "addressable". If an implementation specification is "required", the covered entity must implement policies and/or procedures that meet what the implementation specification requires. If an implementation specification is "addressable", then the covered entity must assess whether it is a reasonable and appropriate safeguard in the entity's environment. This involves analyzing the specification in reference to the likelihood of protecting the entity's e-PHI from reasonably anticipated threats and hazards. If the covered entity chooses not to implement the addressable specification based on its assessment, it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure. In this document, a required implementation specification will be indicated by an "(Required)" and an addressable specification will be indicated by an "(Addressable)". Ascend Technologies has assigned several metrics to each one of these standards. For each metric we assign a score of zero to three to indicate how well the organization is performing for that metric. We then combine these metrics to give an overall score for the implementation specification and standard. Many of the HIPAA standards overlap. Many metrics may appear more than once due to this. Using our scoring system Ascend Technologies can provide organizations with an overview of their compliance with the HIPAA Security Rule.

The Office of Civil Rights (OCR) guidance documentation and this report group these standards into three safeguard sections.

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards

Each one of these safeguard sections are broken down into several standards which are further broken down into multiple implementation specifications. An overview of the client's compliance is outlined below

HIPAA Administrative Safeguards

The Security Rule defines Administrative Safeguards as “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information”.

Administrative Safeguards is the largest section of the HIPAA Security Rule. It contains 9 standards, some of which are broken down further into implementation specifications. The standards and implementation specifications are listed below.

1. Security Management Process 164.308(a)(1)
 - a. Risk Analysis (Required)
 - b. Risk Management (Required)
 - c. Sanction Policy (Required)
 - d. Information System Activity Review (Required)
2. Assigned Security Responsibility 164.308(a)(2)
3. Workforce Security 164.308(a)(3)
 - a. Authorization and/or Supervision (Addressable)
 - b. Workforce Clearance Procedure (Addressable)
 - c. Termination Procedures (Addressable)
4. Information Access Management 164.308(a)(4)
 - a. Isolating Health Care Clearinghouse Functions (Required)
 - b. Access Authorization (Addressable)
 - c. Access Establishment and Modification (Addressable)
5. Security Awareness and Training 164.308(a)(5)
 - a. Security Reminders (Addressable)
 - b. Protections from Malicious Software (Addressable)
 - c. Log-in Monitoring (Addressable)
 - d. Password Management (Addressable)
6. Security Incident Procedures 164.308(a)(6)
 - a. Response and Reporting (Required)
7. Contingency Plan 164.308(a)(7)
 - a. Data Backup Plan (Required)
 - b. Disaster Recovery Plan (Required)
 - c. Emergency Mode Operation Plan (Required)
 - d. Testing and Revision Procedures (Addressable)
 - e. Applications and Data Criticality Analysis (Addressable)
8. Evaluation 164.308(a)(8)
9. Business Associate Contracts and Other Arrangements 164.308(b)(1)
 - a. Written Contract or Other Arrangements (Required)

Security Management Process 164.308(a)(1)

The purpose of this standard is to establish the administrative processes and procedures that a covered entity uses to prevent, detect, contain, and correct security violations. Security Management Process has four Implementation Specifications that are all required. The four specifications are Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review

Risk Analysis (Required)

Score: 17 of 24

The Risk Analysis Implementation Specification states an entity must "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

Metric 1: An organization should have documented the location of all e-PHI data and know how this data flows throughout the organization. This includes all locations where data is created, received, maintained or transmitted by the covered entity

Result 1: E-PHI is documented and has known locations. Vendor A is a 3rd party vendor with ABC that facilitates transmission of e-PHI with several other vendors ABC Company uses. Servers containing PHI are in locked secure room. PHI box is locked in this room too. Any PHI in OneDrive is stored encrypted at rest.

Result 1 Score: 3 of 3

Metric 2: An Organization should deploy an automated inventory discovery tool and use it to build a preliminary asset inventory of systems connected to the enterprise network. Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed

Result 2: Internally, equipment is asset tagged. Tool A logs clients. Mobile device management through O365 enterprise licensing.

Result 2 Score: 2 of 3

Metric 3: Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine names(s), purpose of each system, an asset owner responsible for each device and the department associated with each device. The inventory should include every system that has an IP address on the network including, but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls etc.), printers, storage area networks, VOIP telephones etc.

Result 3: Tool A manages the inventory. ABC Company gets a report each month from Security Vendor on activity.

Result 3 Score: 3 of 3

Metric 4: Secure the asset inventory database and related systems, ensuring that they are included in periodic vulnerability scans and that asset information is encrypted. Limit access to these systems to authorized personnel only, and carefully log all such access. For additional security, a secure copy of the asset inventory may be kept in an offline system air-gapped from the production network.

Result 4: Tool B in Cloud Service which is managed by the developer. MFA for all accounts accessing Tool B. Limited access is established to authorized personnel.

Result 4 Score: 3 of 3

Metric 5: Machines running legacy OS's or Software which cannot be updated due to business reasons should be properly air-gapped.

Result 5: No legacy systems present in environment.

Result 5 Score: 3 of 3

Metric 6: Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses

Result 6: Installations require administrator override, mobile device policy states what programs are acceptable and not acceptable. Authorization required for out of band application.

Result 6 Score: 3 of 3

Metric 7: Organizations should run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis. Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability scanning tool. Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours.

Result 7: No automated vulnerability scanning is being utilized at this time.

Result 7 Score: 0 of 3

Metric 8: In order to overcome limitations of unauthenticated vulnerability scanning, organizations should ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on each end point to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

Result 8: No automated vulnerability scanning is being utilized at this time.

Result 8 Score: 0 of 3

Risk Analysis Overall Score: 17 of 24

Risk Management (Required)

Score: 7 of 15

The Risk Management Implementation Specification states an entity must “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).”

Metric 1: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.

Result 1: ABC Company has a domain that requires DA to join WIFI and LAN network.

Result 1 Score: 3 of 3

Metric 2: Deploy application whitelisting technology that allows systems to run only approved software and prevents execution of all other software on the system, based on an automatically generated list of valid software from a representative sample machine. Such whitelisting tools must be based on acceptable hashing algorithms for determining authorized binaries to execute on a system.

Result 2: No application whitelisting is currently being utilized. Local-admin rights are needed for installations.

Result 2 Score: 1 of 3

Metric 3: Strict configuration management should be followed, building a secure image that is used to build all new systems that are deployed to the enterprise. Any existing system that becomes compromised is re-imaged with the secure build. Regular updates to this image are integrated into the organization's change management processes.

Result 3: No image build. Everything is OS install then Tool B software and configuration installations.

Result 3 Score: 0 of 3

Metric 4: Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system, such as those released by NIST, NSA, Defense Information Systems Agency (DISA), Center for Internet Security (CIS), and others. This hardening would typically include removal of unnecessary accounts, disabling or removal of

unnecessary services, and configuring non-executable stacks and heaps through the use of operating system features such as data execution prevention (DEP). Such hardening also involves, among other measures, applying patches, closing open and unused network ports, implementing Intrusion Detection Systems and/or intrusion prevention systems, and erecting host-based firewalls

Result 4: No image build is being utilized.

Result 4 Score: 0 of 3

Metric 5: Continuous monitoring should be performed on outbound traffic. Any large transfers of data or unauthorized encrypted traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.

Result 5: Security Tools perform these functions. These products are managed by Security Vendor for ABC Company.

Result 5 Score: 3 of 3

Risk Management Overall Score: 7 of 15

Sanction Policy (Required)

Score: 12 of 12 (Excellent)

The Sanction Policy Implementation Specification states and entity must "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

Metric 1: The entity is required to have a security policy which includes language relating to violations of these policies.

Result 1: This is outlined in policy section 3 and 4 of the documentation provided by ABC Company.

Result 1 Score: 3 of 3

Metric 2: The security policy should have examples of potential violations of the security policy.

Result 2: Examples are provided of violations in policy sections 3 and 4 of the ABC HIPAA plan provided.

Result 2 Score: 3 of 3

Metric 3: The security policy should have disciplinary action based upon the severity and procedures.

Result 3: Escalated disciplinary actions are outlined within the security policy. 1st verbal warning, 2nd write up and training, 3rd retraining, 4th, all the above plus management board including termination.

Result 3 Score: 3 of 3

Metric 4: Signed statement(s) of adherence to security policies and acknowledgement that violation of the security policies may lead to disciplinary action is required for all employees.

Result 4: Documented on HIPAA policies. This is documented in the Workforce Member HIPAA Compliance and Confidentiality Statement that all workforce members are required to sign. Custody of these signed policies are maintained by ABC Company.

Result 4 Score: 3 of 3

Sanction Policy Overall Score: 12 of 12 (Excellent)

Information System Activity Review (Required)

Score: 12 of 21

The Information System Activity Review Implementation Specification states and entity must “implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.” Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the damage done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files

Metric 1: All remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism), should be logged verbosely

Result 1: Tool A devices do have event logging. The logs are not offloaded or centralized. Any log investigation or analysis happens on the Tool A.

Result 1 Score: 1 of 3

Metric 2: Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions. Failed log-on attempts must also be logged.

Result 2: Failed logon attempts, lockout at 3 attempts. Servers are mapped by Security Vendor to allow user access. OneDrive access is handled at administration level. Exceeding failed logon attempts are logged. Audit logs for AD services, user events are accessible.

Result 2 Score: 3 of 3

Metric 3: Each organization should include at least two synchronized time sources (i.e., network time protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Result 3: NTP servers located on the domain servers, at least two NTP are used.

Result 3 Score: 3 of 3

Metric 4: Network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, should be configured to verbosely log all traffic (both allowed and blocked) arriving at the device.

Result 4: Tool A security center does log for allowed and blocked traffic.

Result 4 Score: 3 of 3

Metric 5: For all servers, organizations should ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.

Result 5: No syslog server is utilized. Everything is self-contained and logs are investigated or analyzed from the local device.

Result 5 Score: 0 of 3

Metric 6: Organizations should deploy a SIEM system tool for log aggregation and consolidation from multiple machines and for log correlation and analysis. Standard government scripts for analysis of the logs should be deployed and monitored. Customized local scripts should also be used.

Result 6: No SIEM solution is deployed or implemented.

Result 6 Score: 0 of 3

Metric 7: Organizations should have a policy and procedure on how, when and what logs and system information are reviewed.

Result 7: Alerts, reporting from the security center. Daily, weekly, monthly reporting. No official policy or procedure. Policy 17 and 28 in the ABC HIPAA Plan reference this as well.

Result 7 Score: 2 of 3

Information System Activity Review Overall Score: 12 of 21

Assigned Security Responsibility 164.309(a)(2)

Score: 6 of 6

The purpose of this standard is to identify who will be operationally responsible for assuring that the covered entity complies with the Security Rule. There are no separate implementation specifications for this standard. The person or group responsible is comparable to the privacy rule (154.530(a)1) Privacy Official. The Security Official and Privacy Official can be the same person.

Metric 1: The organization is required to clearly identify the person(s) responsible for the Security Rule

Result 1: Executive A and Director of compliance and quality, Director B are identified as the Privacy and Security officer. IT consultant and Security Vendor is retained for their IT management services.

Result 1 Score: 3 of 3

Metric 2: The organization needs to clearly identify and document the roles and responsibilities the person(s) identified responsible for the HIPAA security rule complies with the security rule

Result 2: Roles and responsibilities are noted in the ABC HIPAA Plan under policy 15. Policy 17 of the same plan outlines auditing of workforce members.

Result 2 Score: 3 of 3

Assigned Security Responsibility Overall Score: 6 of 6

Security Management Process 164.308(a)(3)

The Workforce Security Standard states that an entity must “Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard], and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information.”

Within a covered entity's environment, workforce members that need access to e-PHI to carry out their duties must be identified. The entity must identify the e-PHI that is needed, when it is needed and make reasonable efforts to control access to the e-PHI. There are 3 addressable implementation specifications in the Workforce Security Standard, Authorization and/or Supervision, Workforce Clearance Procedure and Termination Procedures

Authorization and/or Supervision (Addressable)

Score: 6 of 6

The Authorization and/or Supervision Implementation Specification states an entity must “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.”

Metric 1: Organizations should have detailed job descriptions for all persons who have access to e-PHI. These descriptions should be used to determine the level of access the person holding the position should have.

Result 1: Role-based Access Control (RBAC) is utilized. PHI access logging analysis is done annually at a minimum. Any point of access the PHI based on their role. Vendor A has audit capability. Access must be approved by Vendor A admin and reviewed by ABC Company. Separation between admin and user. Policy 47 in the ABC HIPAA plan outlines the access controls for each level.

Result 1 Score: 3 of 3

Metric 2: An entity should identify a person that can make decisions on who can and what level access is granted.

Result 2: Leadership channels decide who gets access to what information. Access is decided internally, Vendor A executes internal decisions for access.

Result 2 Score: 3 of 3

Authorization and or Supervision Overall Score: 6 of 6

Workforce Clearance Procedure (Addressable)

Score: 6 of 6

The Workforce Clearance Implementation Specification states an entity should “Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.”

Metric 1: The entity should have documented the procedures for determining the appropriate access level given to employees.

Result 1: Procedure is documented by Policy 47, 20, and 21 in the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: The entity should consistently follow the documented procedures when granting access for a job position or function.

Result 2: Procedure is documented in Policy 20 and 21 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Workforce Clearance Procedure Overall Score: 6 of 6

Termination Procedures (Addressable)

Score: 7 of 9

“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)”

Metric 1: An entity should have a policy in place to where responsibilities to an individual or group for removing information system and physical access.

Result 1: Policy 22 in provided documentation. Exit procedure checklist as well. Signatures of completion for checklist.

Result 1 Score: 3 of 3

Metric 2: An organization should have a procedure in place for the removal of terminated employees in a timely manner (24 hours or less).

Result 2: Resignations: Last day at 5pm is execution of access removal. Terminated: escorted out of the building and access removal is done within 24 hours. Policy 22 outlines this in the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Metric 3: A review of all system accounts of critical systems should be performed periodically. Any account that cannot be associated with a business process or owner should be disabled.

Result 3: Review of email accounts done annually. Email accounts are manually reviewed. ABC Company is provided monthly reports as well.

Result 3 Score: 1 of 3

Termination Procedures Overall Score: 7 of 9

Information Access Management 164.308(a)(4)

The Information Access Management Standard states and entity must "Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule"

Restricting access to only those persons and entities with a need for access is a basic rule of security. This standard addresses this rule and has three implementation specifications, one required and two addressable. The required implementation specification is Isolating Health Care Clearinghouse Functions. The addressable specifications are Access Authorizations and Access Establishment and Modification.

Isolating Health Care Clearinghouse Functions (Required)

The Isolating Health Care Clearinghouse Functions require "If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the e-PHI of the clearinghouse from unauthorized access by the larger organization"

This rule applies only to healthcare clearinghouses that are part of a larger organization. They are not a clearinghouse and this section is not applicable.

Access Authorizations (Addressable)

Score: 21 of 21 (Excellent)

The Access Authorizations Implementation Specification requires an entity to “Implement policies and procedures for granting access to e-PHI, for example through access to a workstation, transaction, program, process, or other mechanism”.

Where this implementation standard is reasonable and appropriate, safeguards must be placed to limit access to e-PHI based upon job function or responsibilities. Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks. In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and ex-filtrate important information with little resistance. In several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data.

Metric 1: An organization should document all authorization to e-PHI documented.

Result 1: Authorization to e-PHI is documented and Leadership is the only entity to grant that authorization. Policy 20 and 21 in the ABC HIPAA Plan outlines this.

Result 1 Score: 3 of 3

Metric 2: An organization should have policies for granting access consistent with the Privacy Rule?

Result 2: Leadership is the only entity at ABC Company authorized to grant access. Policy 20 and 21 in the ABC HIPAA Plan outlines this as well.

Result 2 Score: 3 of 3

Metric 3: Access rules should be applied based upon the level of access required. Employees with different job functions should have separate levels of access based upon their job function.

Result 3: RBAC is utilized and implemented for all jobs. Minimum standards and training required to access PHI. Policy 9 outlines this as well in the ABC HIPAA Plan.

Result 3 Score: 3 of 3

Metric 4: Organizations should ensure that file shares have defined controls (such as Windows share access control lists) that specify at least that only "authenticated users" can access the share

Result 4: Local shares for server, scheduling drive is mapped access. Access to scheduling drive requires domain credentials and authorized access to local shares. Authorization again is provided only by Leadership. OneDrive shares are tiered access or designated need to know.

Result 4 Score: 3 of 3

Metric 5: The network should be segmented based on the trust levels of the information stored on the servers. Whenever information flows over a network of lower trust level, the information should be encrypted

Result 5: OneDrive shares are tiered accessor designated by need to know.

Result 5 Score: 3 of 3

Metric 6: All access should be individualizing. All shared logins for critical devices and assets containing e-PHI should be eliminated.

Result 6: No shared logins, all access is individually based on role.

Result 6 Score: 3 of 3

Metric 7: The use of portable USB drives should either be limited or data should automatically be encrypted before it is written to a portable drive.

Result 7: Policy requires prohibits regular USB usage, only company provided USB may be used. Policy 39 of the ABC HIPAA Plan outlines this. Any PHI stored on a USB will be disposed of after use if the information is sensitive, using one of the outlined methods of destruction.

Result 7 Score: 3 of 3

Access Authorizations Overall Score: 21 of 21 (Excellent)

Access Establishment and Modification (Addressable)

Score: 9 of 9 (Excellent)

The Access Establishment and Modification Implementation Specification suggests entities, "Implement policies and procedures that, based upon the entity's access authorization policies, establishes, document, review and modify a user's right of access to a workstation, transaction, program or process"

Metric 1: An organization should have a policy in place for creating and modifying access to information systems.

Result 1: Leadership dictates all access and modifications of access. Policy 20 and 21 document this in the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: An organization should have these policies documented and updated as necessary.

Result 2: These are documented in policy 20 and 21 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Metric 3: Review all system accounts and disable any account that cannot be associated with a business process and owner

Result 3: Accounts are disabled and removed once confirmation of non-association or requirement is established.

Result 3 Score: 3 of 3

Access Establishment and Modification Overall Score: 9 of 9 (Excellent)

Security Awareness and Training 164.308(a)(5)

The Security Awareness and Training Standard states an entity must "Implement a security awareness and training program for all members of its workforce (including management)."

Any organization that hopes to be ready to find and respond to attacks effectively owes it to its employees and contractors to find the gaps in its knowledge and provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved and can also help determine proper allocation of limited resources to improve security practices.

Training is also closely tied to policy and awareness. Policies tell people what to do, training provides them the skills to do it, and awareness changes behaviors so that people follow the policy. Training should be mapped against the skills required to perform a given job. If after training, users are still not following the policy, that policy should be augmented with awareness.

This Standard has 4 addressable implementation specifications, Security Reminders, Protection from Malicious Software, Log-in Monitoring and Password Management.

Security Reminders (Addressable)

Score: 12 of 12

The Security Reminders Implementation Specification states an entity must implement "Periodic Security Updates." This can be as simple as notices in printed or electronic form up to formal training.

Metric 1: Organizations should develop security awareness training for various personnel job descriptions. The training should include specific, incident-based scenarios showing the threats an organization faces and should present proven defenses against the latest attack techniques.

Result 1: Security awareness has multiple tiers. Healthcare Compliance, everyone is required to complete this for annual training. Workforce members are required to do internal training, created by Executive A and Director B. Miscellaneous training is done throughout the year. Ancillary materials are provided in the environment. Screensavers are security awareness training aides as well. Deficiencies are addressed with newsletter, presentations, emails.

Result 1 Score: 3 of 3

Metric 2: Awareness should be carefully validated with policies and training. Policies tell users what to do, training provides them the skills to do it, and awareness changes their behavior so that they understand the importance of following the policy.

Result 2: First healthcare compliance is used as a security awareness standardized platform. Privacy and security rules form the framework for the security awareness training.

Result 2 Score: 3 of 3

Metric 3: Metrics should be created for all policies and measured on a regular basis. Awareness should focus on the areas that are receiving the lowest compliance score.

Result 3: Employees must pass with 85% score, or the training is not considered passed and completed. Workforce members will have to repeat the training until they pass. First healthcare compliance is utilized for testing.

Result 3 Score: 3 of 3

Metric 4: Organizations should devise periodic security awareness assessment quizzes to be given to employees and contractors on at least an annual basis in order to determine whether they understand the information security policies and procedures, as well as their role in those procedures.

Result 4: No internal testing is directly conducted by ABC Company; however, a document of acknowledgement is required. Healthcare compliance provides metric based testing/quizzing.

Result 4 Score: 3 of 3

Security Reminders Overall Score: 12 of 12

Protection from Malicious Software (Addressable)

Score: 22 of 24

Organizations where appropriate should have "Procedures for guarding against, detecting, and reporting malicious software".

Malicious software is an integral and dangerous aspect of Internet threats, targeting end users and organizations via web browsing, e-mail attachments, mobile devices, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as antimalware tools, help defend against these threats by attempting to detect malware and block its execution.

Metric 1: Organizations should employ automated tools to monitor workstations, servers, and mobile devices for active, anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers

Result 1: Several security tools are all deployed in the environment or are managed by Security Vendor for ABC Company.

Result 1 Score: 3 of 3

Metric 2: Organizations should employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update

Result 2: Anti-malware and signatures are automatically updated. Services are cloud based.

Result 2 Score: 3 of 3

Metric 3: Organizations should configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

Result 3: Auto-run is disabled on all endpoints.

Result 3 Score: 3 of 3

Metric 4: Organizations should configure systems so that they conduct an automated antimalware scan of removable media when it is inserted.

Result 4: Security Tool will scan removable media for malicious content.

Result 4 Score: 3 of 3

Metric 5: All attachments entering the organization's e-mail gateway should be scanned and blocked if they contain malicious code or file types unneeded for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes email content filtering and web content filtering.

Result 5: O365 enterprise is used. 3rd-party scan service does sandbox. A daily quarantine report is provided.

Result 5 Score: 3 of 3

Metric 6: Automated monitoring tools should use behavior-based anomaly detection to complement and enhance traditional signature-based detection.

Result 6: Security Tools perform automated monitoring.

Result 6 Score: 3 of 3

Metric 7: Organizations should deploy network access control tools to verify security configuration and patch-level compliance before granting access to a network

Result 7: Tool A performs patching.

Result 7 Score: 3 of 3

Metric 8: Continuous monitoring should be performed on outbound traffic. Any large transfers of data or unauthorized encrypted traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.

Result 8: This is provided by the Tool A for outbound traffic.

Result 8 Score: 1 of 3

Protection from Malicious Software Overall Score: 22 of 24

Log-in Monitoring (Addressable)

Score: 6 of 9

The Log-in Monitoring implementation Specification states the covered entity must implement "Procedures for monitoring log-in attempts and reporting discrepancies"

Metric 1: Systems should automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.

Result 1: Security Vendor reports provide this information. Device spotlights referenced in the report signifies failed login attempts.

Result 1 Score: 3 of 3

Metric 2: After eight failed log-on attempts within a 45-minute period, the account should be locked for 120 minutes.

Result 2: This is documented in Policy 28 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Metric 3: Organizations should configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group.

Result 3: This is not currently alerted or alarmed on for DA group changes.

Result 3 Score: 0 of 3

Log-in Monitoring Overall Score: 6 of 9

Password Management (Addressable)

Score: 18 of 27

The covered entity must implement "Procedures for creating, changing and safeguarding passwords".

METRIC 1: To prevent brute force attacks and easily guessed passwords, all accounts should be required to have a minimum length of 12 characters and contain at least 3 of 4 of upper case letters, lower case letters, numbers, and special characters.

RESULT 1: Password changes minimum of twice a year. At least 7 characters, one number and one symbol. Workforce members are accountable for their password changes.

Result 1 Score: 1 of 3

METRIC 2: Organizations should configure operating systems so that passwords cannot be reused within a certain timeframe, such as six months.

RESULT 2: Passwords can be reused after every 3rd password reset.

Result 2 Score: 1 of 3

METRIC 3: Before deploying any new devices in a networked environment, organizations should change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.

RESULT 3: Specific username and passwords on deployed devices are used instead of default.

Result 3 Score: 3 of 3

Metric 4: Organizations should configure all administrative-level accounts to require regular password changes on a frequent interval of no longer than 60 days. All service-level accounts to require regular password changes on a frequent interval of no longer than 90 days

Result 4: Every 6 months for email, automatic password changes for service level and admin required at 90 days.

Result 4 Score: 3 of 3

Metric 5: Organizations should segregate administrator accounts based on defined roles within the organization. For example, "Workstation admin" accounts should only be allowed administrative access of workstations, laptops, etc.

Result 5: Everyone has their own workstation; administrator accounts are based on role. There are no segmented workstations just for administrator accounts or administrative tasks.

Result 5 Score: 1 of 3

Metric 6: Through policy and user awareness, organizations should require that administrators establish unique, different passwords for their administrator and non-administrative accounts. Each person requiring administrative access should be given his/her own separate account. Administrative accounts should never be shared. Users should only use the Windows

"administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrator accounts.

Result 6: Security Vendor has administrator login and only has the one account.

Result 6 Score: 2 of 3

Metric 7: All administrative access, including domain administrative access, should use two factor authentication.

Result 7: Two factor is not required for local workstation login but does have two-factor for email administrator.

Result 7 Score: 1 of 3

Metric 8: If services are outsourced to third parties, language should be included in the contracts to ensure that they properly protect and control administrative access. It should be validated that they are not sharing passwords and have accountability to hold administrators liable for their actions.

Result 8: Vendors and partners sign that said vendor/partner will protect any asset utilized for conducting business with ABC. Vendors are vetted and a checklist process is used. Policy 6 of the ABC HIPAA Plan outlines this.

Result 8 Score: 3 of 3

Metric 9: An organization should implement policies to not share passwords or logins. Passwords should be committed to memory and not written down in areas visible to others.

Result 9: Policy 21 in the ABC HIPAA Plan established this.

Result 9 Score: 3 of 3

Password Management Overall Score: 18 of 27

Security Incident Procedures 164.308(a)(6)

The Security Incident Procedure Standard states that covered entities must "Implement policies and procedures to address security incidents."

Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response plans in place. Without an incident response plan, an organization may not discover an attack

in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.

This Standard only has one Implementation Specification, Response and Reporting, which is required.

Response and Reporting (Required)

Score: 12 of 12

This specification states that covered entities must "Identify and respond to suspected of 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"

Metric 1: Organizations should ensure that they have written incident response procedures that include a definition of personnel roles for handling incidents. The policies should list the possible types of security incidents and the response for each

Result 1: Policy 30 defines the Incident Response and the contingency plan is outlined in policy 31.

Result 1 Score: 3 of 3

Metric 2: Organizations should assign job titles and duties for handling computer and network incidents to specific individuals.

Result 2: Policy 30 of the ABC HIPAA Plan describes and outlines titles and duties for an incident response.

Result 2 Score: 3 of 3

Metric 3: Organizations should define management personnel who will support the incident handling process by acting in key decision-making roles

Result 3: Policy 30 of the ABC HIPAA Plan defines support personnel. Leadership and possible 3rd party consulting.

Result 3 Score: 3 of 3

Metric 4: Organizations should devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate US Community Emergency Response Team in accordance with all government requirements for involving that organization in computer incidents

Result 4: ABC Company has a non-defined timeframe. Immediate notification is outlined in policy 30. 3 business days maximum allowed. Policy 4 and 5 supplement this as well.

Result 4 Score: 3 of 3

Response and Reporting Overall Score: 12 of 12

Contingency Plan 164.308(a)(7)

The Contingency Plan standard requires that covered entities “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 damage systems that contain electronic protected health information”

The Contingency Plan Standard has 5 implementation specifications. The required specifications are Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan. The addressable specifications are Testing and Revision Procedures and Applications and Data Criticality Analysis.

Data Backup Plan (Required)

Score: 15 of 15 (Excellent)

The Data Backup Plan specification requires covered entities to “Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information”

Metric 1: Organizations backup plan should include all important sources of data such as patient accounting systems, electronic medical records, health maintenance and case management information.

Result 1: Policy 32 of the ABC HIPAA Plan addresses this. The secure server backed up. PHI is stored and physical stored if downloaded.

Result 1 Score: 3 of 3

Metric 2: Organizations should ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. However, each must be backed up at least weekly

Result 2: Server is backed up on hourly basis or daily basis. There is a tertiary failover of servers should the redundant server fail. ABC Company has local backups and cloud-based backups.

Result 2 Score: 3 of 3

Metric 3: Organizations should ensure that backups are properly protected via physical security or encryption when they are stored locally, as well as when they are moved across the network.

Result 3: Sign in sheet on inner room, secure room. The room is restricted access. The room is mechanically secured room by lock. Executive A has one key and spare key is in lockbox. Policy 32 of the ABC HIPAA Plan supplements this as well.

Result 3 Score: 3 of 3

Metric 4: Data backups should be stored in a secured offsite location close enough to facilitate a timely restore of data when required, but far enough to lessen the dangers of a natural disaster such as tornado, fire or flood destroying both the primary and backup data.

Result 4: Datto uses AES 256 and SSL key-based encryption to secure all data during transmission and storage. That includes the data "at rest" in both local and cloud-based backups, as well as the data in transit to Datto's data centers and back.

Result 4 Score: 3 of 3

Metric 5: Transfer and storage of backup data should be done securely. Backups should be transferred and stored via encryption.

Result 5: Datto uses AES 256 and SSL key-based encryption to secure all data during transmission and storage. That includes the data "at rest" in both local and cloud-based backups, as well as the data in transit to Datto's data centers and back.

Result 5 Score: 3 of 3

Data Backup Plan Overall Score: 15 of 15

Disaster Recovery Plan (Required)

Score: 12 of 12 (Good)

The Disaster Recovery Plan is a required specification that has entities "Establish (and implement as needed) procedures to restore any loss of data"

Metric 1: Key personnel should be trained on both the backup and restoration processes. To be ready in case a major incident occurs, alternative personnel should also be trained on the restoration process just in case the primary IT point of contact is not available.

Result 1: Executive A and Director B would handle the local level actions, notify upper management, contact building manager. For anything beyond Executive A or Director B , they would contact Security Vendor for 3rdparty assistance. Policy 32 of the ABC HIPAA Plan outlines the disaster recovery plan and backup plan.

Result 1 Score: 3 of 3

Metric 2: Disaster Recovery Plans should not be a generic plan. It should be customized to an organization's operating environment.

Result 2: Policy 32, outlines the disaster recovery plan. Covers numerous natural disasters and provides contact points, roles, responsibilities for employees.

Result 2 Score: 3 of 3

Metric 3: The organizations Disaster Recovery plan should address what data is to be restored.

Result 3: Security Vendor would help make that determination. Policy 35 of the ABC HIPAA Plan outlines application and criticality.

Result 3 Score: 3 of 3

Metric 4: The Disaster Recovery Plan should be updated, stored and readily available at more than one location.

Result 4: A Local copy is kept onsite; a copy of the policies is kept up in OneDrive. The disaster plan is reviewed annually.

Result 4 Score: 3 of 3

Disaster Recovery Plan Overall Score: 12 of 12

Emergency Mode Operation Plan (Required)

Score: 6 of 6

The Emergency Mode Operation Plan specification is required and mandates that covered entities to "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.”

Metric 1: An organization should keep a plan for emergency operation mode which should include phone numbers, contact names, roles and responsibilities of all persons involved in the emergency process in the event of disaster.

Result 1: Policy 34 in the ABC HIPAA Plan outlines this.

Result 1 Score: 3 of 3

Metric 2: When an organization is operating under emergency conditions, the protection of the e-PHI must be maintained. The Emergency mode operation plan should specify how it will maintain these protections while also maintaining access to the data.

Result 2: ABC Company limits access to PHI during emergency or disaster. PHI maintained in the cloud, still secure. Designated workforce members would be based on role and responsibility in regard to access of PHI.

Result 2 Score: 3 of 3

Emergency Mode Operations Plan Overall Score: x of 6 (Poor)

Testing and Revision Procedures (Addressable)

Score: 10 of 12

The Testing and Revision Procedures is an addressable specification that states reasonable and appropriate safeguards for a covered entity to “Implement procedures for periodic testing and revision of contingency plans.”

METRIC 1: Data on backup media should be tested on a regular basis by performing a data restoration process to ensure that the backup is properly working

RESULT 1: This is outlined in policy 31 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

METRIC 2: Individuals responsible for emergency response and disaster recovery need to understand their responsibilities.

RESULT 2: Responsibilities are outlined in policy 32 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

METRIC 3 : Data Organizations should perform routine walk-through or complete live tests of their emergency response and disaster recovery

RESULT 3 : This is described in policy 32 of the ABC HIPAA Plan.

Result 3 Score: 2 of 3

METRIC 4 : Entities should record results from tests and update their procedures to correct any problems encountered.

RESULT 4 : This process is outlined in policy 32 of the ABC HIPAA Plan.

Result 4 Score: 2 of 3

Testing and Revision Procedures Overall Score: 10 of 12

Applications and Data Criticality Analysis (Addressable)

Score: 3 of 3

Data on backup media should be tested on a regular basis by performing a data restoration process to ensure that the backup is properly working. The Applications and Data Criticality Analysis specification is an addressable specification mandating entities to "Assess the relative criticality of specific applications and data in support of other contingency plan components."

METRIC 1 : An entity's Emergency Operation Mode and Disaster Recovery Plan should prioritize the applications and data required for patient care and business needs.

RESULT 1 : This is outlined and described in policy 32 and 35 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Applications and Data Criticality Analysis Overall Score: 3 of 3

Evaluation 164.308(a)(8)

Score: 6 of 6

Security plans and procedures only work if they are kept current. Failure to monitor and update plans can lead to gaps in coverage, data compromises and/or delays in access to much needed information.

The Evaluation Standard is a required standard with no separate implementation specification that addresses updating of policies and plans. It states that entities "Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations 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 [the Security Rule]." This Assessment and report cover a majority of this standard.

METRIC 1 : The security plans should be evaluated periodically, when security incidents are identified, changes are made in the organization or new technology is implemented

RESULT 1 : This process is outlined in policy 36 and 45 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

METRIC 2 : Assessments should be a combination of internal and external evaluations and the results should be incorporated into the security plan

RESULT 2 : This is noted in policy 36 and 45 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Evaluation Overall Score: 6 of 6

Business Associate Contracts and Other

A growing vector for e-PHI compromises is through the business associations of an organization. An organization can be in perfect compliance with the HIPAA security rule, but a business partner may not be. The latest HIPAA guidelines stipulate that any partner an entity shares e-PHI with must also be HIPAA compliant.

The Business Associate Contracts and Other Arrangements Standard has one required implementation specification, Written Contract or Other Arrangement

Written Contract or Other Arrangement (Required)

Score: 6 of 6

Cover entities are required to: "Document the satisfactory assurances required by paragraph (b)(1) [The business associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of 164.314(a)"

Metric 1: An organization is required to identify and document all business associates that create, receive, maintain or transmit e-PHI information on behalf of the organization.

Result 1: Any partner or business associate are kept on file. If the relationship ends, the contact is removed. Further information is found in policy 6 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: An Organization is required to contractually address a business associate's compliance with the Privacy Rule that involves e-PHI.

Result 2: BAA addresses the contractual compliance for the privacy Rule for any business associate. Policy 6 of the ABC HIPAA Plan addresses this.

Result 2 Score: 3 of 3

Written Contracts or Other Arrangements Overall Score: 6 of 6

Physical Safeguards

The Security Rule defines physical safeguards as “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Physical Safeguards is the smallest section of the HIPAA Security Rule. It contains 4 standards, some of which are broken down further into implementation specifications. The standards and implementation specifications are listed below.

1. Facility Access Controls 164.310(a)(1)
 - a. Contingency Operations (Addressable)
 - b. Facility Security Plan (Addressable)
 - c. Access Control and Validation Procedure (Addressable)
 - d. Maintenance Records (Addressable)
2. Workstation Use 164.310(b)
3. Workstation Use 164.310(c)
4. Device and Media Control 164.310(d)(1)
 - a. Disposal (Required)
 - b. Media Re-use (Required)
 - c. Accountability (Addressable)
 - d. Data Backup and Storage (Addressable)

Facility Access Controls 164.310(a)(1)

“Implement policies and procedures to limit physical access to its electronic housed, information systems and the facility or facilities in which they are while ensuring that properly authorized access is allowed.”

Contingency Operations (Addressable)

Score: 6 of 6

A covered entity must “Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency”

Metric 1: Organizations should keep a list of workforce personnel that have been identified as needing physical access in an emergency.

Result 1: This is outlined in policy 32 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: Organizations must have access to facilities to restore data in the event of an emergency such as power outage. Confirmation that key workforce personnel will have this access should be verified.

Result 2: Server backups provides this restore access. Policy 32 of the ABC HIPAA Plan outlines these items.

Result 2 Score: 3 of 3

Contingency Operations Overall Score: x of 6 (Excellent)

Physical Security Plan (Addressable)

Score: 9 of 9

The entity must "Implement policies and procedures to safeguard the facility and the equipment there in from unauthorized physical access, tampering and theft."

Metric 1: Entities need to have controls in place to physically restrict access to where e-PHI can be accessed and/or stored. Examples of controls are locked doors, cameras and warning signs

Result 1: These restrictions are in policy 37 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: Where reasonable and appropriate, monitoring of access should be employed. Examples include security guards, recording cameras, badges and personal security codes.

Result 2: Building has security guard, security cameras in parking garage and outside of the office door (48-hour loops), building owned. Office space entry is by electronic keypad and Ring doorbell system. Auditing of keypad access is accessible to ABC. Internal office keypad is ADT alarm system.

Result 2 Score: 3 of 3

Metric 3: Organizations should have written policies in place stating that all e-PHI data will be stored in a physically secure location such as the controls listed in the first couple metrics.

Result 3: Policy 37 of the ABC HIPAA covers this.

Result 3 Score: 3 of 3

Physical Security Plan Overall Score: 9 of 9

Access Control and Validation Procedure (Addressable)

Score: 9 of 12

The covered entity must "Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

Metric 1: Organizations should have policy in place that validates a person's access to facilities based on their function

Result 1: Office electronic keypad access is only given to workforce members.

Result 1 Score: 3 of 3

Metric 2: Organizations should control the person's access to facilities. Examples include guards, identification badges or keypads.

Result 2: Building has security guard, security cameras in parking garage and outside of the office door (48-hour loops), building owned. Office space has an electronic keypad and Ring doorbell system. Auditing of keypad access is accessible to ABC. Internal office keypad is ADT alarm system.

Result 2 Score: 3 of 3

Metric 3: Organizations should identify vendors or non-required personnel needing access to the areas containing e-PHI, such as requiring them to sign in, wear visitor badges and/or be escorted by authorized personnel

Result 3: Vendors or business associates are to be escorted and only allowed to an entrance area. Courier only person allowed to be in PHI lockbox area, bound by BAA with ABeo. Lock bags are used for transporting any Billing sheets or PHI information.

Result 3 Score: 3 of 3

Metric 4: Organization Management should regular review the list of persons who have physical access to the facilities housing e-PHI data.

Result 4: A specific list of workforce members is not maintained or reviewed.

Result 4 Score: 0 of 3

Access Control and Validation Procedures Overall Score: 9 of 12

Maintenance Records (Addressable)

Score: 1 of 6 (Poor)

The covered entity must “Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).”

Metric 1: An entity should have policies to specify how to document repairs to the physical infrastructure of the facilities housing e-PHI data.

Result 1: Physical infrastructure repairs are outsourced to an individual.

Result 1 Score: 1 of 3

Metric 2: An entity should have policies and documentation that specify what physical components which require documentation when repairs are made.

Result 2: The ABC HIPAA Plan does not have a policy outlining this.

Result 2 Score: 0 of 3

Maintenance Records Overall Score: 1 of 6 (Poor)

Workstation Use 164.310(b)

Score: 15 of 15

The Workstation Use Standard defines a workstation as “an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.”

This required standard states that entities must develop policies that specify the proper functions to be performed by electronic devices. The Workstation Use Standard states that entities must “Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. There are no Implementation Specifications with this standard

METRIC 1 : An organization must have a written policy in place that specifies the proper functions to be performed on workstations that access e-PHI.

RESULT 1 : This is outlined in policy 38 and 39 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

METRIC 2 : An organization must have in place policies that identify workstations that can access EPHI and those that do not.

RESULT 2 : This is outlined in policy 21, 38 and 39 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

METRIC 3 : An Organization must have in place policies that address a workstations physical placement to allow viewing by only authorized individuals

RESULT 3 : This is outlined in policy 39 and 40 of the ABC HIPAA Plan.

Result 3 Score: 3 of 3

METRIC 4 : Organizations should have written policies in place on the use of additional security measures to protect e-PHI such as privacy screens, password protected screen savers and logging off of workstations.

RESULT 4 : These policies are outlined in policy 40 of the ABC HIPAA Plan.

Result 4 Score: 3 of 3

METRIC 5 : Policies should be in place addressing workstation use for users that access e-PHI from remote locations

RESULT 5 : Policy 41 of the ABC HIPAA Plan dictates how mobile devices access e-PHI.

Result 5 Score: 3 of 3

Workstation Use Overall Score: 15 of 15

Workstation Security 164.310(c)

Score: 9 of 9

The Workstation Security Standard requires an entity to “Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”

The Workstation Use Standard states how the workstation is to be use. This step expands on that and addresses how a workstation is to be protected from unauthorized access. This is a required standard that has no Implementation Specifications.

METRIC 1: An entity is required to implement physical safeguards that restrict access to authorized users on workstations that access e-PHI

RESULT 1: Laptops require being locked in drawer, locked office doors and locked workstations. Policy 41 of the ABC HIPAA Plan also supplements this metric.

Result 1 Score: 3 of 3

METRIC 2: An entity needs to have all types of workstations identified that access e-PHI. Examples include laptops, desktops, tablets, phones or other PDAs.

RESULT 2: This is outlined in policy 38 and 39 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

METRIC 3: Are the Physical Safeguards used to protect workstations documented in the Workstation Use policies and procedures.

RESULT 3: This is outlined in policy 38 and 40 of the ABC HIPAA Plan.

Result 3 Score: 3 of 3

Workstation Security Overall Score: 9 of 9

Device and Media Control 164.310(d)(1)

The Device and Media Control Standard requires entities to “Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic

protected health information, into and out of a facility, and the movement of these items within the facility.”

The standard defines electronic media as “electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium such as magnetic tape or disk, optical disk, or digital memory card”

The Device and Media Control Standard has four Implementation Specifications, two required and two addressable. The required specifications are Unique User Identification and Emergency Access Procedure. The address specifications are Automatic Logoff and Encryption and Decryption

Disposal (Required)

Score: 6 of 6

The covered entity must “Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware of electronic media on which it is stored”

Metric 1: An entity should have policies implemented that addresses disposal of e-PHI and the hardware/electronic media it is stored on.

Result 1: This is outlined in policy 39 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: The policies should address the process to make the e-PHI unusable or inaccessible. Specifications on what technology such as software or specialized piece of hardware should be stated within the policy

Result 2: This is outlined in policy 39 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Disposal Overall Score: 6 of 6

Media Re-use (Required)

Score: 6 of 6

The Media Re-use Implementation Specification states the entity must “Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.”

This implementation specification deals with the re-use of electronic media instead of disposal.

Metric 1: There should be a policy in place addressing the removal of e-PHI from electronic media that is to be reused.

Result 1: Policy 39 of the ABC HIPAA Plan addresses this.

Result 1 Score: 3 of 3

Metric 2: The policy should stipulate how the e-PHI is removed and in what situation from the electronic media prior to reuse. In most cases this should be reformatting and/or completely erasing the entire electronic media

Result 2: Policy 39 of the ABC HIPAA Plan addresses this.

Result 2 Score: 3 of 3

Media Re-Use Overall Score: 6 of 6

Accountability (Addressable)

Score: 6 of 6

The Accountability Implementation Specification states that an entity should "Maintain a record of movements of hardware and electronic media and any person responsible therefore."

Metric 1: A record of all e-PHI containing electronic media should be kept. This record should include the hardware type, serial numbers, person(s) responsible, and information regarding the movement of the individual electronic media. This includes hard drives, magnetic tapes, optical disks or digital memory cards.

Result 1: Inventory of all the hardware is recorded. Workforce members are only allowed to use authorized devices.

Result 1 Score: 3 of 3

Metric 2: An entity should have a policy stating the process when to create, modify or delete a record for e-PHI containing electronic media.

Result 2: Policy 42 of the ABC HIPAA Plan addresses this.

Result 2 Score: 3 of 3

Accountability Overall Score: 6 of 6

Data Backup and Storage (Addressable)

Score: 3 of 3

The Data Backup and Storage Implementation Specification states the entity must "Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

This specification is similar to the Contingency Plan Standard of the Administrative Safeguard. These specifications often cover the same policies and procedures. Due to many of the metrics already being covered in that section, this section only covers the situation of equipment movement.

Metric 1: A policy should be in place to identify the situations and the persons responsible for creating retrievable exact copies of e-PHI when needed before movement of equipment

Result 1: Policy 43 of the ABC HIPAA Plan outlines this metric.

Result 1 Score: 3 of 3

Data Backup and Storage Overall Score: 3 of 3

Technical Safeguards

Technical Safeguards is the last section of the HIPAA Security Rule. It contains 5 standards, some of which are broken down further into implementation specifications. The standards and implementation specifications are listed below.

1. Access Control 164.312(a)(1)
 - a. Unique User Identification (Required)
 - b. Emergency Access Procedure (Required)
 - c. Automatic Logoff (Addressable)
 - d. Encryption and Decryption (Addressable)
2. Audit Controls 164.312(b)
3. Integrity 164.312(c)(1)
 - a. Mechanism to Authenticate Electronic PHI (Addressable)
4. Person or Entity Authentication 164.312(d)
5. Transmission Security 164.312(e)(1)
 - a. Integrity Controls (Addressable)
 - b. Encryption (Addressable)

Access Control 164.312(a)(1)

The Access Control Standard requires a covered entity to "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."

The Access Control has four implementation specifications. 2 are required and are Unique User Identification and Emergency Access Procedures. 2 are addressable and are Automatic Logoff and Encryption and Decryption.

Unique User Identification (Required)

Score: 6 of 6

The Unique User Identification Implementation Specification states the entity must "Assign a unique name and/or number for identifying and tracking user identity."

Metric 1: An organization's workforce members should have a unique identifier that follows a standard format.

Result 1: First initial and last name are how employees are uniquely identified.

Result 1 Score: 3 of 3

Metric 2: An organization's unique identifier system should be used to track user activity within the e-PHI system.

Result 2: first initial last name is the unique identifier. Policy 40 provides guidance on this.

Result 2 Score: 3 of 3

Unique User Identification Overall Score: 6 of 6

Emergency Access Procedure (Required)

Score: 6 of 6

The Emergency Access Procedure Implementation Specification states the entity must "Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency"

Metric 1: An organization must determine who needs access to the e-PHI in the event of an emergency.

Result 1: This is outlined in policy 32 of the ABC HIPAA Plan.

Result 1 Score: 3 of 3

Metric 2: There should be policies in place to provide appropriate access to e-PHI in emergency situations.

Result 2: This is addressed in policy 31 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Emergency Access Procedure Overall Score: 6 of 6

Automatic Logoff (Addressable)

Score: 6 of 6

The Automatic Logoff Implementation Specification states the entity must "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"

Metric 1: All systems that contain e-PHI should have automatic logoff capabilities and it should be enabled. A benchmark of 10 minutes is recommended.

Result 1: Automatic logoff is enabled. Policy states immediate locking of workstations when workforce member is away from the workstation. Automatic logoff is set to 10 minutes.

Result 1 Score: 3 of 3

Metric 2: All workstations that access e-PHI should have an automatic logoff or screen locking capability and it should be enabled. A benchmark of 10 minutes is recommended.

Result 2: Automatic logoff is enabled. Policy states immediate locking of workstations when workforce member is away from the workstation. Automatic logoff is set to 10 minutes. Screensaver locking is enabled as well.

Result 2 Score: 3 of 3

Automatic Log Off Overall Score: 6 of 6

Encryption and Decryption (Addressable)

Score: 17 of 18

The Encryption and Decryption Implementation Specification states the entity must “Implement a mechanism to encrypt and decrypt electronic protected health information”

Metric 1: All remote administration of servers, workstations, network devices, and similar equipment should be done over secure channels. Protocols such as telnet, virtual network computing (VNC), remote desktop protocol (RDP), or other protocols that do not natively support strong encryption should only be used if they are performed over a secondary encryption channel, such as secure sockets layer (SSL) or Internet protocol security (IPSEC).

Result 1: VNC utilizing http over SSL is utilized in the environment.

Result 1 Score: 2 of 3

Metric 2: All web applications that transmit e-PHI should perform such transfers over an encrypted link such as SSL

Result 2: Any phi is transmitted through Vendor A securely. Mail encryption platform is used for secure email.

Result 2 Score: 3 of 3

Metric 3: An organization must have all Wi-Fi that transmits e-PHI be secured using advanced encryption standard (AES) encryption with Wi-Fi Protected Access 2 (WPA2) protection.

Result 3: WIFI uses least AES and WPA2-PSK.

Result 3 Score: 3 of 3

Metric 4: Organizations should ensure that backups are properly protected via physical security or encryption when they are stored locally, as well as when they are moved across the network.

Result 4: All backups are encrypted at rest and encrypted when in transmission across the network.

Result 4 Score: 3 of 3

Metric 5: The use of portable USB drives should either be limited or data should automatically be encrypted before it is written to a portable drive

Result 5: Use of USB drives is limited and controlled. Policy 39 of the ABC HIPAA Plan outlines how USB or flash drives employed at ABC Company.

Result 5 Score: 3 of 3

Metric 6: Organizations should deploy approved hard drive encryption software to mobile machines that hold sensitive data.

Result 6: Endpoint encryption is used for hard drive encryption. IOS devices are naturally encrypted.

Result 6 Score: 3 of 3

Encryption and Decryption Overall Score: 17 of 18

Audit Control 164.312(b)

Score: 13 of 15

The Audit Control Standard is a required standard that states an entity must "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information".

The Audit Control Standard as no implementation specifications. This standard is similar to the Administrative Safeguards=Security Management Process=Information System Activity Review. Many of the same metrics are used.

Metric 1: Network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, should be configured to verbosely log all traffic (both allowed and blocked) arriving at the device

Result 1: Local logging enable on all edge devices. No retention of logs is currently done.

Result 1 Score: 2 of 3

Metric 2: For all servers, organizations should ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.

Result 2: Event logs are not collected or not written to any centralized or dedicated logging server.

Result 2 Score: 2 of 3

Metric 3: Each organization should include at least two synchronized time sources (i.e., network time protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Result 3: Two NTP time sources are used in the environment.

Result 3 Score: 3 of 3

Metric 4: Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions. Failed log-on attempts must also be logged.

Result 4: Security Vendor reports provide this information. Device spotlights referenced in the report signifies failed login attempts.

Result 4 Score: 3 of 3

Metric 5: All remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism), should be logged verbosely

Result 5: Tool A generates these logs.

Result 5 Score: 3 of 3

Audit Control Overall Score: 13 of 15

Integrity 164.312(c)(1)

The Integrity Standard requires an entity to "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

This standard has one addressable implementation standard, Mechanism to Authentication Electronic PHI.

Mechanism to Authenticate Electronic PHI (Addressable)

Score: 0 of 3

The entity must “Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner”.

Metric 1: All e-PHI devices that store e-PHI should employ automatic checks for data integrity such as check sum verification or digital signatures.

Result 1: No FIM or data integrity monitoring is done locally.

Result 1 Score: 0 of 3

Mechanism to Authenticate Electronic PHI Overall Score: 0 of 3

Person or Entity Authentication 164.312(d)

Score: 1 of 3

The entity must “Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed”

Metric 1: An entity needs to implement an authentication mechanism that verifies the user is who they claim they are.

Result 1: Two factor authentication is used for email. No workstation usage or login requires two factor authentication.

Result 1 Score: 1 of 3

Person or Entity Authentication Overall Score: 1 of 3

Transmission Security 164.312(e)(1)

The final standard is Transmission Security. This standard stipulates an entity “Implement technical security measures to guard against unauthorized access electronic protected health information that is being transmitted over an electronic communications network.”

This standard has 2 addressable implementation specifications, Integrity Controls and Encryption.

Integrity Controls (Addressable)

Score: 6 of 6

The entity must "Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of"

Metric 1: An entity is required to transmit all e-PHI in a secure manner.

Result 1: This is accomplished through Vendor A. Policy 47 and 43 in the ABC HIPAA Plan expand on this.

Result 1 Score: 3 of 3

Metric 2: Organization should assess how e-PHI data is transmitted and how securely the transmission is on regular intervals.

Result 2: This is addressed in Policy 43, 47 and 40 of the ABC HIPAA Plan.

Result 2 Score: 3 of 3

Integrity Controls Overall Score: 6 of 6

Encryption (Addressable)

Score: 3 of 3

The Encryption Implementation Specification states an entity must "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

Metric 1: To ensure that e-PHI is not being compromised during transmission, an organization should transmit all traffic securely using a strong encryption protocol.

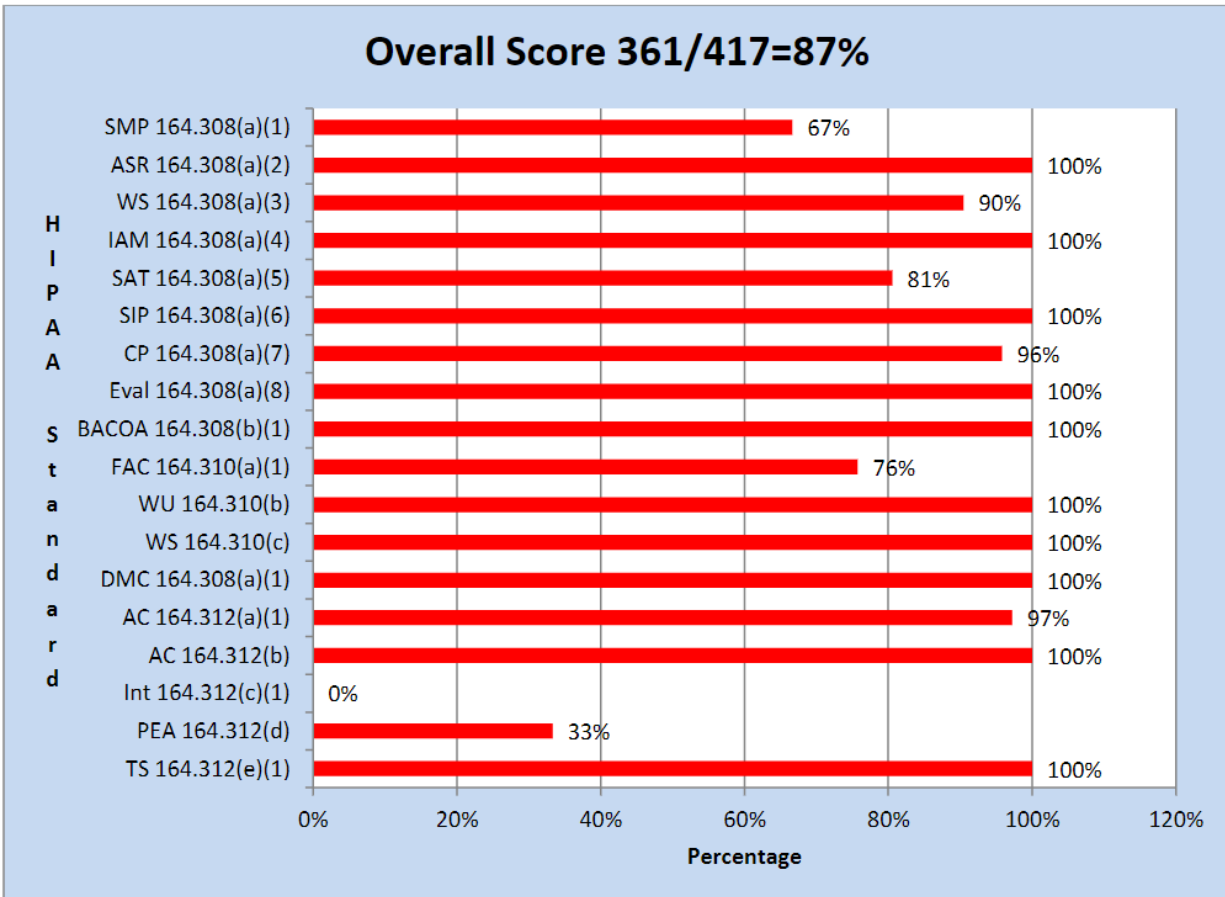
Result 1: Electronic PHI is encrypted in transit and when at rest. Policy 43, 47 and 40 of the ABC HIPAA Plan outlines this.

Result 1 Score: 3 of 3

Encryption Overall Score: 3 of 3 (Excellent)

Critical Controls Overall Score

Overall Score: **361 of 417, 87%**



Vulnerability Assessment

Ascend Technologies performed a vulnerability scan of ABC Company's internal networks using Qualys. A full vulnerability report is included as an addendum to this document.

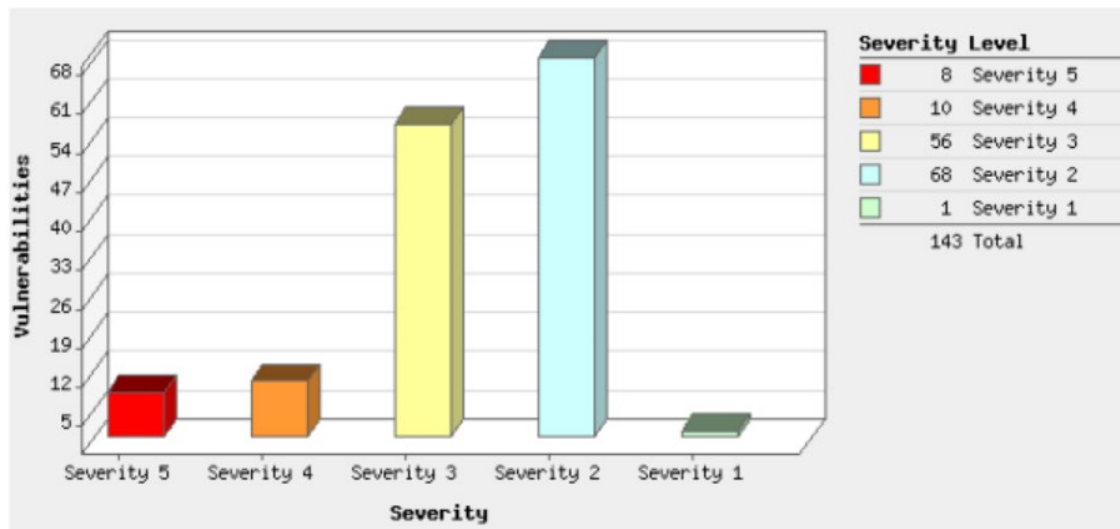
A vulnerability scan is used to identify assets on the network at risk to compromise due to insecure configuration or missing updates. Scanning is used to determine only vulnerabilities or potential vulnerabilities on systems by accessing listening services and analyzing responses to queries in order determine vulnerability status.

Summary of Results

Vulnerabilities are classified on a scale of 1 to 5. With 5 being the most critical and 1 being innocuous. Our scanning identified 154 confirmed severity 5 vulnerabilities, and 98 confirmed severity 4 vulnerabilities. Severity 4 and 5 vulnerabilities should be addressed immediately as they generally indicate remotely exploitable vulnerabilities that an attack could use to gain control of a device.






The illustration below represents a summary of the overall vulnerability status of ABC COMPANY'S internal group of networks.

Vulnerabilities by Severity



Of the 143 vulnerabilities identified, 8 are severity 5, mainly associated with EOL software on printers and web server software. 10 severity 4 vulnerabilities were mainly from outdated software like jQuery and OpenSSH. Though not as severe as level 5 vulnerabilities, level 4 are considered critical and can provide attackers full access to information stored on the network host. A vulnerability is a design flaw or misconfiguration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vendors release periodic patches to fix software design flaws. It is important to implement these patches soon after they are released.

Below is a detailed explanation of the vulnerability security levels:

Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Most discovered vulnerabilities fall under the informational category. These vulnerabilities can be remediated by reviewing security configurations on devices and changing default settings and accounts. Severity 3's can be remediated by signing SSL certificates and disabling access to protocols if possible (i.e., disable SSLv3 and TLSv1.0). It is important to implement both vulnerability and patch management solutions to automate the discovery and tracking of vulnerable systems, and then in turn, mitigate the vulnerabilities by deploying patches to affected systems.

Based on the results of the vulnerability scans it is apparent that there is still a need for a vulnerability management solution and any remediation processes should continue. Having an effective vulnerability scanner to scan for threats that are not detected by patch management is very important. Uncommon 3rdparty software and insecure configurations are not assessed by patch management solutions and often go unnoticed or overlooked by IT personnel. Regular reviews of these reports should be conducted, and any severity four or five vulnerabilities should be addressed in a timely fashion. If it cannot be mediated for any reason, it should be documented, and appropriate security measures should be implemented to contain any threats these vulnerabilities pose to systems.

Recommendations

There are a large number of security related items, both positive and negative, outlined in this document. We fully suggest reading the entirety of the document to help in developing your own strategic security plan. Below are some high-level suggestions that we recommend for addressing the most critical risks in the ABC COMPANY environment.

- Implement a Vulnerability Assessment and Management program. This includes adding regular internal vulnerability scanning in addition to external vulnerability scanning. Additionally, having policies and metrics in place for remediation and measuring effectiveness of this specific program is also important.
- File Integrity Monitoring detects changes made to files and systems. This can detect and alert to unauthorized changes made to identified sensitive information or systems. Implementing a solution for FIM can help identify security threats both internal and externally.
- A central logging solution combined with a SEIM solution will enhance troubleshooting, reporting and analysis of security and operational events more efficiently and can be tied to automated alerting and reporting.
- Two Factor Authentication (2FA) or multi-factor authentication for workstations that have access to sensitive information or e-PHI is recommended. MFA provides an additional authentication layer at a local level and provides another layer of security should a user account and password be compromised.

Conclusions

ABC Company has talented and educated IT and management staff with Security Vendor. Many core security policies and technologies have already been effectively implemented at ABC Company largely due to HIPAA. The network appears to be well designed and includes segmentation to protect the network from pivoting in the event of a compromised host.

The leadership at ABC Company are savvy and have done a lot of work implementing security policies and procedures. Much of the technology already exists in the network to properly defend it. Enacting and enforcing policies and procedures is the other side of that coin. Continuing evaluation and updating of established policies and procedures will keep the work already done in a current state and actionable for items like incident response or disaster recovery.

