HIPAA and HITECH Act

Compliance Guide

Updated March 2013

What is HIPAA and the HITECH Act?

Like most other industries, healthcare is moving away from paper processes to rely more heavily on the use of electronic information systems. Electronic resources are used to pay claims, answer eligibility questions, provide health information, and to conduct a host of other administrative and clinically based functions. Health plans are now providing access to claims and care management, as well as self-service applications for members. The rise in the adoption rate of these new technologies comes with a rise in potential security risks.

In this context, the **Health Insurance Portability and Accountability Act (HIPAA)**, administered by the US Department of Health and Human Services, makes its mark by mandating that patient medical records and other healthcare information be protected against security breaches and unauthorized use or disclosure while stored, processed, and exchanged between healthcare organizations and parties such as insurance companies, healthcare providers, pharmacies, employers, and patients.

The Health Information Technology for Economic and Clinical Health (HITECH) Act has clarified and supplemented HIPAA requirements, particularly by raising the financial penalties in cases of non-compliance.

Who must be HIPAA compliant?

Any healthcare organization that stores, processes, or transmits personal health information is considered a **covered entity** and is required to adhere to the Privacy and Security Rules of the HIPAA.

This includes:

- Covered healthcare providers (hospitals, clinics, regional health services, individual medical practitioners) that conduct certain transactions in electronic form
- Healthcare clearinghouses (entities that help healthcare providers and health plans standardize their information
- Health plans (insurers, HMOs, Medicaid, Medicare prescription drug card sponsors, flexible spending accounts, public health authority, and employers, schools or universities that collect, store or transmit PHI to enroll employees or students in health plans)
- Any covered business associates (including private sector vendors and third-party administrators) must also adhere to the rules. The HIPAA rules define "business associate" generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. The term "business associate" also includes health information organizations, e-prescribing gateways or others that provide data transmission services with respect to protected health information to a covered entity and that require routine access to the health information. A business associate can also include those who offer a personal health record to one or more individuals on behalf of a covered entity. **Note**: Subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate are also considered to be business associates.

» Note: Guidance on how to determine whether an entity is a covered entity under the HIPAA is available **here**.

Who is responsible for HIPAA compliance?

The Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) are responsible for administering, enforcing, and validating these standards and may conduct compliance investigations and reviews.

The HIPAA audit

At this time, all covered entities are eligible to be subject to auditing. The OCR is responsible for selection of the entities that will be audited.

The OCR is expected to notify selected covered entities between 30 and 90 days prior to the anticipated onsite visit. Onsite visits may take between 3 and 10 business days depending upon the complexity of the organization and the auditor's need to access materials and staff. After fieldwork is completed, the auditor will provide the covered entity with a drafted final report. The covered entity will then have 10 business days to review and provide written comments back to the auditor. The auditor will complete a final audit report within 30 business days after the covered entity's response and submit it to the OCR.

» The OCR HIPAA Audit Protocol can be accessed **here**.

What are the consequences of non-compliance?

Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. There are four tiers of increasing penalty amounts that correspond to the levels of culpability associated with a HIPAA violation. The minimum fines range between $100 and $50,000 per violation, and are capped at $1.5 million for all violations of the same HIPAA provision during any calendar year (see below table). The lowest category of violation covers situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of the HIPAA violation. The second lowest category of violation applies to violations due to reasonable cause and not to willful neglect. "reasonable cause" meaning here "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated [HIPAA], but in which the covered entity or business associate did not act with willful neglect." By "willful neglect" one means the "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA.

The third category applies to situations where the violation was due to willful neglect and was corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation. The fourth category applies to situations where the violation was due to willful neglect and not corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation.

Breach notification

HHS issued regulations requiring healthcare providers, health plans, and other entities covered by the HIPAA to notify individuals when their health information is breached.

In this context, the term “breach” means: The acquisition, access, use, or disclosure of protected health information in a manner not permitted by the “Privacy rules” which compromises the security or privacy of the protected health information which means “poses a significant risk of financial, reputational, or other harm to the individual.”

Regulations developed by the OCR require that healthcare providers and other HIPAA covered entities promptly notify affected individuals of a breach. The HHS Secretary and the media must also be promptly notified in cases where a breach affects more than 500 individuals. The Act requires that these notifications are made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity if they experience a breach.

What is the HIPAA Compliance Framework?

There are two specific regulations of interest to covered entities: the HIPAA Privacy Rule and the HIPAA Security Rule. They are explained below.

The **Privacy Rule** defines and limits the circumstances in which individual identifiable health information may be used or disclosed by covered entities. This information includes demographic data such as name, address, birth date, Social Security Number and information that relates to:

- The individual’s past, present, or future physical or mental health or condition
- The provision of healthcare to the individual
- The past, present, or future payment for the provision of healthcare to the individual

The Privacy Rule calls this information Protected Health Information (PHI).

However, some data are excluded from protected health information, such as employment records that a covered entity maintains in its capacity as an employer, education records, and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

The Privacy Rule is NOT specific to electronic information and applies equally to written records, telephone conversations, etc. It mandates that organizations may only release PHI as explicitly permitted by the Privacy Rule or with the prior written consent of the individual who is the subject of the records. The Privacy Rule also contains a number of notification and administrative requirements designed to ensure proper records are maintained, and that individuals are aware of their rights under HIPAA.

The **Security Rule** covers the protection of the confidentiality, integrity, and availability of electronic protected health information (ePHI). It prescribes a number of required policies, procedures, and reporting mechanisms that must be in place for all information systems that process, store, and transmit ePHI within and between covered entities.

> *» Note: The scope of the Security Rule is more limited than that of the Privacy Rule. The Privacy Rule applies to protected health information (PHI) in any form, whereas this rule applies only to protected health information in electronic form (ePHI).*

The Security Rule contains multiple proposed requirements (or standards) and implementation specifications designed to protect the confidentiality, integrity and availability of ePHI within each enterprise. These specifications fall into five categories:

1. Administrative Safeguards (§164.308)

2. Physical Safeguards (§164.310)
3. Technical Safeguards (§164.312)
4. Organizational Requirements (§164.314)
5. Policies and Procedures (§164.316)

> *» Note: Because the speed with which technology is evolving could make specific requirements obsolete and might deter technological progress, the Security Rule has been written to frame the requirements (standards) in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.*

How can organizations comply with HIPAA?

The Security Rule lists a set of security requirements (standards) along with a list of related *required* or *addressable* implementation specifications.

“Required” specifications *must* be implemented.

“Addressable” specifications must be implemented if deemed “reasonable and appropriate” by the covered entity.

A covered entity must decide whether a given “addressable” security measure is reasonable and appropriate to apply within its particular security framework. Each entity must make individual business decisions about how security requirements will be satisfied and which technology will be used. Each decision will depend on a variety of factors, such as the entity’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

Based upon each decision, the following applies for addressable specifications:

- If a security measure is deemed reasonable and appropriate, the covered entity must implement it.
- For situations where inappropriate and/or unreasonable security measures have been identified for a standard that must be met, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. The decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard must be documented.
- For situations where security measures aren’t applicable to a certain standard, the covered entity must document the decision to not implement the addressable specification, the rationale behind that decision, and how the standard is being met.

How Rapid7 can help

Rapid7 has extensive experience partnering with healthcare service providers (such as BlueCross BlueShield of Vermont, Memorial Sloan-Kettering Cancer Center, and the Spectrum Health System) to help them with the complex regulatory environment of the health sector.

Rapid7 provides full end-to-end security solutions and services for healthcare entities to help them meet HIPAA compliance using security standards and specific implementations outlined in the Security Rule.

Rapid7 Nexpose is a security risk intelligence solution that proactively supports the entire vulnerability management lifecycle including discovery, detection, verification, risk classification, impact analysis, reporting, and mitigation.

In the context of the HIPAA, Nexpose helps covered entities to:

- Detect ePHI data in their environment.
- Get top-down visibility of risk to their assets and business operations, enabling them to organize and prioritize thousands of assets and quickly focus on the items that pose the greatest risk.
- Get a clear map of the real risk posed to their ePHI by the identified vulnerabilities across the healthcare organization's IT landscape. Nexpose is the only product that includes real exploit and malware intelligence combined with CVSS base scores, temporal scoring, environmental considerations (e.g., any mitigating controls in place), and asset criticality for risk classification.
- Take inventory of their systems, services, and installed applications using the latest fingerprinting technologies.
- Detect the presence of unauthorized software on organizational information systems and notify designated organizational officials through alerts on an automated mechanism.
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications.
- Generate easy-to-use detailed reports combined with role-based access controls to allow organizations to share information easily.
- Compare the results of vulnerability scans over time to determine trends in information system vulnerabilities through an automated mechanism.
- Audit users and groups on their systems.
- Discover accounts that were terminated and review results either in the UI or in report format, and then use the data to influence information access and management policies.
- Set up automated monitoring access controls (including adherence to policies for role-based access) to validate enforcement of access restrictions.
- Test the efficiency of their access control systems and policies.

- Test external and internal boundaries defenses.
- Detect and report malicious software.
- Set up automated monitoring access controls including limiting the number of login attempts, password length requirements, allowable special characters, and other login ID access control policies.
- Get a detailed, sequenced remediation roadmap with time estimates for each task, which can then be managed either through Nexpose's built-in ticket system or through a leading help desk system such as Remedy, Peregrine, Tivoli, or CA.
- Support incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits.
- Ensure continuous logging of historical scan data showing a device's previous state.
- Use automated utilities to save duplicates of data to a backup server.
- Deliver auditable and reportable events on vulnerabilities throughout the infrastructure.
- Provide records about the sources of events, outcomes of events related to vulnerabilities, and details of what occurred in any given event.

Rapid7 Metasploit Pro is a penetration testing solution that helps enterprise vulnerability management programs test how well their perimeter holds up against real world attacks.

In the context of the HIPAA, Metasploit Pro helps covered entities to:

- Test the efficiency of their access control systems and policies.
- Survey hosts for use of approved authentication measures.
- Audit password length/complexity and authentication methods.
- Test external and internal boundaries defenses.
- Support incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits.
- Perform external and internal penetration testing to determine if a hacker could access and steal ePHI. Penetration testing includes network-layer and application-layer tests. Penetration testing is conducted using Nexpose in conjunction with a variety of specialized tools including Metasploit, the leading open-source penetration testing platform with the world's largest database of public, tested exploits.

Rapid7 Consulting Services help covered entities to:

- Perform formal risk assessments and assist in writing documentation to meet HIPAA standards.
- Conduct a vulnerability analysis on information systems.
- Perform penetration testing on information systems based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

- Perform a full gap analysis including penetration testing and social engineering to evaluate daily security controls, determine if security policies are being followed in actual day-to-day operations, identify gaps in a security program, and provide guidance on developing missing control policies and procedures required to secure information systems, ePHI, and data from external threats.

- Recommend best practices to optimize data security, including system access policies that limit access to system components and sensitive data to only those whose job roles absolutely require such access.

- Provide customizable security awareness training to users of organizational information systems.

- Provide vulnerability management security training and certification to managers and users of organizational information systems requiring knowledge and technical abilities to detect and validate vulnerabilities on IT infrastructure, determine the associated risk severity, write IT risk reports, and apply mitigations through remediation and control.

- Audit recovery plans to identify any gaps that should be addressed in order to successfully backup and restore systems, and establish procedures to ensure business process continuity and private protection while operating in emergency mode.

- Perform an independent analysis and penetration test against delivered information systems, information system components, and information technology products.

The Rapid7 community, SecurityStreet, helps covered entities to:

- Stay up-to-date with the latest developments in the vulnerability management and information security areas.

Security Rule standards	Nexpose	Metasploit	Consulting Services
Administrative safeguard			
Security management process (§ 164.308.a.1)	●		●
Assigned security responsibility (§ 164.308.a.2)			
Workforce security (§ 164.308.3)	●		●
Information access management (§ 164.308.a.4)	●	●	●
Security Awareness Training (§ 164.308.a.5)	●	●	●
Security incident procedures (§ 164.308.a.6)	●	●	●
Contingency plan (§ 164.308.a.7)	●		●
Evaluation (§ 164.308.a.8)	●	●	●
Business associate contracts and other arrangements (§ 164.308.b.1)			
Physical safeguard			
Facility access controls (§ 164.310.a.1)			●
Workstation use (§ 164.310.a.2)			●
Workstation security (§ 164.310.a.3)			●
Device and media controls (§ 164.310.a.4)			●
Technical safeguard			
Access control (§ 164.312.a.1)	●		●
Audit controls (§ 164.312.a.2)	●		●

Integrity (§ 164.312.a.3)			●
Person or entity authentication (§ 164.312.a.4)	●		●
Transmission security (§ 164.312.a.5)			●
Organizational requirements			
Business associate contracts or other arrangements (§ 164.314.a.1)			●
Requirements for group health plans (§ 164.314.a.2)			●
Policies, procedures and documentation requirements			
Policies and procedures (§ 164.316.a.1)			●
Documentation (§ 164.316.a.1)			●

Rapid7 Solution for HIPAA Compliance

This section goes into detail about the Security Rule requirements/standards, required (R) or addressable (A) implementation specifications, and how Rapid7 Nexpose, Metasploit Pro, and Consulting Services help covered entities become HIPAA compliant.

Administrative Safeguard (§ 164.308)

(§ 164.308.a.1) Security management process – Implement policies and procedures to prevent, detect, contain, and correct security violations

- Identify relevant information systems
- Conduct a risk assessment
- Acquire IT systems and services
- Create and deploy policies and procedures

Associated implementation specifications:

A	Risk analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity.	R
B	Risk management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	R
C	Sanction policy	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	R
D	Information system activity review	Implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports	R

Use Rapid7 Nexpose to:

- Detect ePHI data in your environment by allowing file searching, so that if Nexpose gains access to an asset's file system in the scanning process it can search for and retrieve files in that system.
- Get top-down visibility of risk to your assets and business operations, enabling your healthcare institution to organize and prioritize thousands of assets and quickly focus on the items that pose the greatest risk.
- Get a clear map of the real risk posed to your ePHI by the identified vulnerabilities across your healthcare organization's IT landscape. Nexpose is the only product that includes real exploit and malware intelligence combined with CVSS base scores, temporal scoring, environmental considerations (e.g., any mitigating controls in place), and asset criticality for risk classification.
- Take inventory of your systems, services, and installed applications using the latest fingerprinting technologies.

- Detect the presence of unauthorized software on organizational information systems and notify designated organizational officials through alerts on an automated mechanism.
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications.
- Generate easy-to-use detailed reports combined with role-based access controls to allow organizations to share information easily.
- Provide an automated mechanism to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Use Rapid7 Consulting Services to:

- Perform formal risk assessments and assist in writing documentation to meet HIPAA standards.
- Conduct a vulnerability analysis on information systems.
- Perform penetration testing on information systems based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.
- Perform a full PCI gap analysis, including penetration testing and social engineering to evaluate your daily security controls, determine if security policies are being followed in actual day-to-day operations, identify gaps in your security program, and provide guidance on developing missing control policies and procedures required to secure information systems and data from external threats.

(§ 164.308.a.2) Assigned security responsibility – Identify the security official who is responsible for the development and implementation of the policies and procedures required for the entity.

- Select a security official to be assigned responsibility for HIPAA security
- Assign and document the individual's responsibilities

Associated implementation specifications:

A	Select a Security Official To Be Assigned Responsibility for HIPAA Security	Assign responsibility for the HIPAA security to a Security Official that will oversee the development, implementation, monitoring, and communication of security policies and procedures.	R
B	Assign and Document the Individual's Responsibilities	Properly document the roles and responsibilities of the assigned individual or organization in a job description and communicate it to the entire organization.	R

(§ 164.308.3) Workforce security - Implement policies and procedures to ensure that all members of a workforce have appropriate access to ePHI, and to prevent workforce members without access from obtaining it.

- Establish clear job descriptions and responsibilities
- Establish criteria and procedures for hiring and assigning tasks
- Establish termination procedures

Associated implementation specifications:

A	Authorization and/or supervision	Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	A
B	Workforce clearance procedure	Implement procedures to determine that the access of a workforce member to ePHI is appropriate.	A
C	Termination procedures	Implement procedures for terminating access to ePHI when the employment of a workforce member ends.	A
D	Establish Clear Job Description and Responsibilities	Formal documentation should identify levels of access to information systems that house ePHI.	A

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure ePHI from external threats

Use Rapid7 Nexpose to:

- Audit users and groups on your systems.
- Discover accounts that were terminated, and review results either in the UI or in report format, and then use the data to influence information access and management policies.

(§ 164.308.a.4) Information access management – Implement policies and procedures for authorizing access to ePHI.

- Determine criteria for establishing access
- Determine who should be authorized to access information systems
- Evaluate existing security measures related to access controls

Associated implementation specifications:

A	Isolating healthcare clearinghouse functions	If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	R
B	Access authorization	Implement policies and procedures for granting access to ePHI through access to a workstation, transaction, program, process, or other mechanism.	A

C	Access establishment and modification	Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.	A
D	Evaluate Existing Security Measures Related to Access Controls	Maintain formal or informal policies and procedures relating to the security measures for access controls. Make sure to approve and update those policies and procedures on a regular basis.	A

Use Rapid7 Nexpose to:

- Leverage your customized policy compliance framework to set up automated monitoring access controls (including adherence to policies for role-based access) to validate enforcement of access restrictions.

Use Rapid7 Metasploit Pro to:

- Test the efficiency of your access control systems and policies.

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure ePHI from external threats.
- Recommend best practices to optimize data security, including system access policies that limit access to system components and sensitive data to only those whose job roles absolutely require such access.

(§ 164.308.a.5) Security awareness and training – Implement a security awareness and training program for all members of a workforce (including management).

- Conduct a training needs assessment
- Develop and approve a training strategy and plan
- Develop appropriate awareness and training content; create training materials; determine best delivery methods
- Implement the training
- Monitor and evaluate training plan

Associated implementation specifications:

A	Develop and Approve a Training Strategy and a Plan	Implement a security awareness and training program addressing the specific required HIPAA policies. The security awareness and training program must outline the scope of the program, be reviewed periodically, and be approved by management. The training materials must incorporate relevant/current IT security topics.	A
B	Implement trainings	Employees must receive all required training to help them fulfill their security responsibilities.	A
C	Monitor and Evaluate Training Plan	Training must be updated and conducted whenever there are changes in the technology and practices.	A
D	Security reminders	Implement periodic security reminders.	A
E	Protection from Malicious Software; Log-in Monitoring; and Password Management	Implement formal or informal policy and procedures to inform employees of the importance of protecting against malicious software and exploitation of vulnerabilities. Those procedures must be updated periodically and approved by management.	A

Use Rapid7 Nexpose to:

- Test your external and internal boundaries defenses.
- Detect and report malicious software
- Set up automated monitoring access controls, including limiting the number of login attempts, password length requirements, allowable special characters, and other login ID access control policies.

Use Rapid7 Metasploit Pro to:

- Survey hosts for use of approved authentication measures.
- Audit password length/complexity and authentication methods.
- Test your external and internal boundaries defenses.

Use Rapid7 Consulting Services to:

- Provide customizable security awareness training to users of your organizational information systems.
- Provide vulnerability management security training and certification to managers and users of organizational information systems requiring knowledge and technical abilities to detect and validate vulnerabilities on the IT infrastructure, determine the associated risk severity, write IT risks reports, and apply mitigations through remediation and control.

Use the Rapid7 community, SecurityStreet, to:

- Stay up-to-date with the latest developments in the vulnerability management and information security areas.

(§ 164.308.a.6) Security incident procedures – Implement policies and procedures to address security incidents.

- Determine goals of incident responses
- Develop and deploy in incident response team
- Incorporate post-incident analysis into updates and revisions

Associated implementation specifications:

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

Use Rapid7 Nexpose to:

- Get a clear map of the real risk posed by the identified vulnerabilities across your organization’s IT landscape. Nexpose is the only product that includes real exploit and malware intelligence combined with CVSS base scores, temporal scoring, environmental considerations (e.g. any mitigating controls in place), and asset criticality for risk classification
- Get a detailed, sequenced remediation roadmap with time estimates for each task, which can then be managed either through Nexpose’s built-in ticket system or through a leading help desk system such as Remedy, Peregrine, Tivoli, or CA.

Use Rapid7 Nexpose and Metasploit Pro to:

- Support incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits.

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure ePHI from external threats

(§ 164.308.a.7) Contingency plan – Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrences (for example: fire, vandalism, system failure, and natural disaster) that damage systems containing ePHI.

- Develop a contingency planning policy
- Conduct an impact analysis
- Identify preventative measures

- Develop recovery strategy
- Develop the contingency plan
- Plan testing, training, and execution

Associated implementation specifications:

A	Data backup plan	Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	R
B	Disaster recovery plan	Establish (and implement as needed) procedures to restore any loss of data.	R
C	Emergency mode operation plan	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	R
D	Testing and revision procedures	Implement procedures for periodic testing and revision of contingency plans.	A
E	Applications and data criticality analysis	Assess the relative criticality of specific applications and data in support of other contingency plan components.	A

Use Rapid7 Nexpose to:

- Ensure continuous logging of historical scan data showing a device's previous state.
- Use automated utilities to save duplicates of data to a backup server.

Use Rapid7 Consulting Services to:

- Audit recovery plans to identify any gaps that should be addressed in order to successfully backup and restore systems, and establish procedures to ensure business process continuity and private protection while operating in emergency mode.

(§ 164.308.a.8) Evaluation – Perform periodic technical and nontechnical evaluations initially based upon the standards implemented under this rule and subsequently as responses to environmental or operational changes that affect the security of ePHI. These periodic evaluations establish the extent to which an entity's security policies and procedures meet the requirements of this subpart.

- Determine whether internal or external evaluation is most appropriate
- Develop standards and measurements for all areas and topics of security
- Conduct evaluation
- Document results
- Repeat evaluations periodically

Associated implementation specifications:

A	Evaluators performance	For evaluations conducted by external consultants, an agreement or contract must exist and include verification of consultants' credentials and experience. For evaluations conducted by internal staff, define the specified performance criteria.	R
B	Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	Implement policy and procedures to ensure an evaluation considers all elements of the HIPAA Security Rule. The process must be approved and updated on a periodic basis.	R
C	Conduct Evaluation	Implement policies and procedures to ensure all necessary information needed to conduct an evaluation is obtained and documented in advance. Policies and procedures must be approved and updated on a periodic basis.	R
D	Document Results	Implement formal or informal policies and procedures to document the evaluation of findings, remediation options and recommendations, and remediation decisions. Written reports of findings must be reviewed and approved by management.	R
E	Repeat Evaluations Periodically	Implement formal or informal security policies and procedures to repeat evaluations when environmental and operational changes are made that affect the security of ePHI. Security policies and procedures must be reviewed on a periodic basis.	R

Use Nexpose in conjunction with Metasploit to:

- Test your external and internal boundaries defenses.

Use Metasploit Pro to:

- Perform external and internal penetration testing to determine if a hacker could access and steal ePHI. Penetration testing includes network-layer and application-layer tests. Penetration testing is conducted using Nexpose in conjunction with a variety of specialized tools including Metasploit, the leading open-source penetration testing platform with the world's largest database of public, tested exploits.

Use Rapid7 Consulting Services to:

- Perform an independent analysis and penetration test against delivered information systems, information system components, and information technology products.

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

(§ 164.308.b.1) Business associate contracts and other arrangements – A covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.

- Identify entities that are business associates under the HIPAA Security Rule
- Execute new agreements or update existing agreements when appropriate
- Establish processes for measuring contract performance and terminating the contract if security requirements are not being met

Associated implementation specifications:

A	Written contract or other arrangement	Document satisfactory assurances through a written contract or other arrangements with business associates that meet the applicable requirements of § 164.314(a)	R

Physical Safeguard (§ 164.310)

(§ 164.310.a.1) Facility access controls - Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- Conduct an analysis of existing physical security vulnerabilities
- Identify corrective measures
- Develop a facility security plan
- Develop access control procedures
- Establish contingency operations procedures

Associated implementation specifications:

A	Contingency operations	Establish (and implement as needed) procedures that allow facility access to support the restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A
B	Facility security plan	Implement policies and procedures to safeguard the facility and the equipment within from unauthorized physical access, tampering, and theft.	A
C	Access control and validation procedures	Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor controls and control of access to software programs for testing and revision.	A
D	Maintenance records	Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).	A

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

(§ 164.310.a.2) Workstation use – 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 ePHI.

- Identify workstation types and functions or uses
- Identify expected performance of each type of workstation
- Analyze physical surrounding for physical attributes

Associated implementation specifications:

A	Identify Workstation Types and Functions or Uses	Implement a process for identifying workstations by type and location. Classify each workstation based on its capabilities, connections, and allowable activities.	R

B	Identify Expected Performance of Each Type of Workstation	Implement formal or informal policies and procedures related to the proper use and performance of workstations. Policies and procedures must be approved and updated on a periodic basis.	R
C	Analyze Physical Surroundings for Physical Attributes	Implement formal or informal policies and procedures to prevent or preclude unauthorized access to an unattended workstation, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed. Policies and procedures must be approved and updated on a periodic basis.	R

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

(§ 164.310.a.3) Workstation security – Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users only.

- Identify all methods of physical access to workstations
- Analyze the risk associated with each type of access
- Identify physical safeguards

Associated implementation specifications:

A	Identify All Methods of Physical Access to Workstations	Physically restrict workstation access to authorized personnel only.	R
B	Identify and Implement Physical Safeguards for Workstations	Implement physical security measures to prevent unauthorized access to restricted information.	R

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

(§ 164.310.a.4) Device and media controls – Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

- Evaluate methods for final disposal of ePHI
- Develop and implement procedures for reuse of electronic media

- Maintain records of hardware, media, and personnel
- Develop backup procedures to ensure that the integrity of ePHI will not be jeopardized during equipment relocation

Associated implementation specifications:

A	Disposal	Implement policies and procedures to address the final disposal of ePHI, and/or the hardware or electronic media on which it is stored.	R
B	Media re-use	Implement procedures for removal of ePHI from electronic media before the media is made available for re-use.	R
C	Accountability	Maintain a record of the movements of hardware and electronic media and the personnel responsible for them.	A
D	Data backup and storage	When needed, create a retrievable and exact copy of ePHI before movement of equipment.	A

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

Technical Safeguards (§ 164.312)

(§ 164.312.a.1) Access control – Implement technical policies and procedures for the electronic information systems that maintain ePHI to only allow access to the persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

- Analyze workloads and operations to identify the access needs of all users
- Identify all data and systems where access control is a requirement
- Ensure that all system users have been assigned a unique identifier
- Develop access control policies
- Implement access control procedures using selected hardware and software
- Review and update user access
- Establish an emergency access procedure
- Terminate access if it is no longer required

Associated implementation specifications:

A	Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.	R
B	Emergency access procedure	Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	R
C	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time period of inactivity.	A
D	Encryption and decryption	Implement a mechanism to encrypt and decrypt ePHI.	A

Use Rapid7 Customized Policy Compliance Framework to:

- Set up automated monitoring access controls, including limiting number of login attempts, password length requirements, allowable special characters, and other login ID access control policies.

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.312.a.2) Audit controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

- Determine activities that will be tracked or audited
- Deploy tracking and reviewing tools
- Implement audit logs

- Regularly review audit records
- Develop review/audit policy and standards.

Associated implementation specifications:

A	Determine the Activities that Will be Tracked or Audited	Implement audit controls over information systems that contain or use ePHI.	R
B	Select the Tools that Will be Deployed for Auditing and System Activity Reviews	Evaluate the audit capabilities of systems and applications and determine whether upgrades are necessary to implement audit capabilities.	R
C	Develop and Deploy the Information System Activity Review/Audit Policy	Implement a formal or informal audit policy to communicate the details of the entity’s audits and reviews to your work force.	R
D	Develop Appropriate Standard Operating Procedures	Implement procedures on the systems and applications to be audited.	R

Use Rapid7 Nexpose to:

- Deliver auditable and reportable events on vulnerabilities throughout the infrastructure.
- Provide records about the sources of events, outcomes of events related to vulnerabilities, and details of what occurred in any given event.

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.312.a.3) Integrity – Implement policies and procedures to protect ePHI from improper alteration or destruction.

- Identify all users who have been authorized to access ePHI
- Identify any possible unauthorized sources that may be able to intercept the information and modify it
- Develop integrity policies and requirements
- Implement procedures to address these requirements
- Establish a monitoring process to assess how the implemented process is working

Associated implementation specifications:

A	Mechanism to authenticate ePHI	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner	A

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.312.a.4) Person or entity authentication – Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

- Determine authentication applicability to current systems/applications
- Evaluate authentication options available
- Select and implement authentication options

Associated implementation specifications:

A	Evaluate Authentication Methods Available	Implement a process to evaluate authentication methods for your systems and applications to assess strengths, weaknesses, and the cost to benefit ratio of different types of authentication in order to establish an appropriate level of authentication.	R
B	Select and Implement Authentication Option	Implement a formal authentication policy for systems and applications. Implement a process to periodically test and upgrade authentication systems.	R

Uses Rapid7 Customized Policy Compliance Framework to:

- Set up automated monitoring access controls (including limiting the number of login attempts, password length requirements, allowable special characters, etc.)

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.312.a.5) Transmission security – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

- Identify any possible unauthorized sources that may be able to intercept and/or modify the information
- Develop a transmission security policy
- If needed, implement procedures for transmitting ePHI using hardware/software.

Associated implementation specifications:

A	Integrity controls	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	A
B	Encryption	Implement a mechanism to encrypt ePHI whenever deemed appropriate	A

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

Organizational Requirements (§164.314)

(§ 164.314.a.1) Business associate contracts or other arrangements – A covered entity is not in compliance with the standards if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangements. The covered entity must have taken reasonable steps to cure the breach or end the violation. If such steps were unsuccessful, the covered entity must have terminated the contract or arrangement if feasible. If termination is not feasible, the covered entity must have reported the problem to the Secretary.

Associated implementation specifications:

A	Business associate contracts	The contract between a covered entity and a business associate must provide that the business associate will: (1) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (2) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (3) Report to the covered entity any security incident of which it becomes aware; (4) Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.	R

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.314.a.2) Requirements for group health plans – A group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI that is created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

Associated implementation specifications:

A	Provision	The plan documents of the group health plan must be amended to incorporate provisions that require the plan sponsor to: (1) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (2) Ensure that the adequate separation is supported by reasonable and appropriate security measures; (3) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; (4) Report to the group health plan any security incident of which it becomes aware.	R

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

Policies, Procedures and Documentation Requirements (§ 164.316)

(§ 164.316.a.1) Policies and procedures - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b).

This standard should not be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time provided that the changes are documented and implemented.

Associated implementation specifications: None

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

(§ 164.316.a.1) Documentation – Maintain the policies and procedures implemented to comply with this subpart in written (may be electronic) form. If an action, activity, or assessment is required by this subpart to be documented, maintain a written (may be electronic) record of the action, activity, or assessment.

Associated implementation specifications:

A	Time limit	Retain the documentation for 6 years from the date of its creation or from the date when it last was in effect, whichever is later.	R
B	Availability	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	R
C	Updates	Review documentation periodically, and update as needed in response to environmental or operational changes affecting the security of the ePHI.	R

Use Rapid7 Consulting Services to:

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

To see how Rapid7's IT Security Risk Management suite can benefit your organization, visit Rapid7.com.