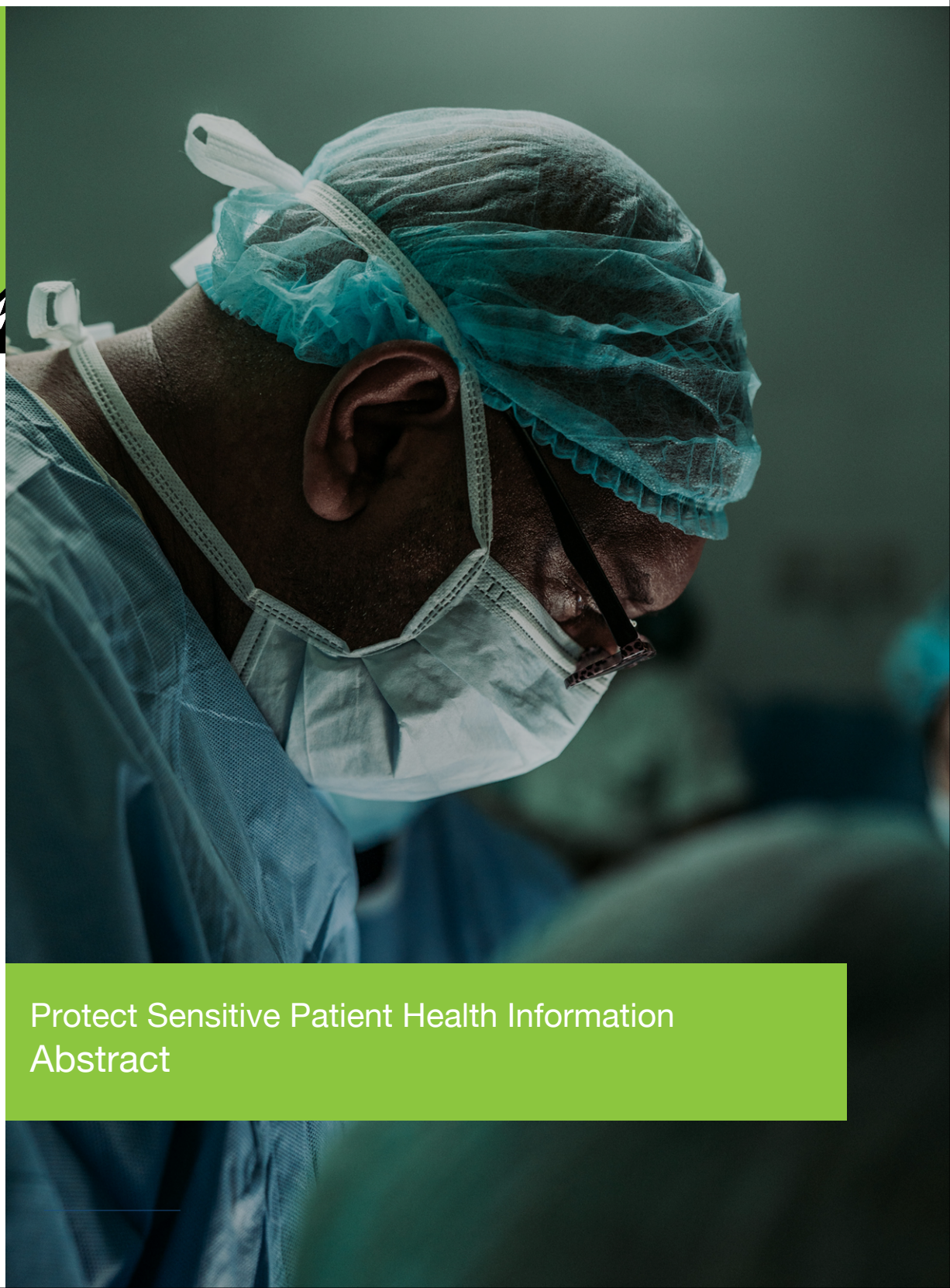
Compliance with the Security for the Healthcare Industry (HIPAA) U.S. Regulation Using RidgeBot

RIDGE SECURITY



Protect Sensitive Patient Health Information

Abstract

Compliance with the Security for the Healthcare Industry (HIPAA) U.S. Regulation Using RidgeBot

Protect Sensitive Patient Health Information

Abstract

This white paper discusses how RidgeBot capabilities—including asset discovery, attack surface identification, iterative security validation, automated and on-demand penetration testing, and vulnerability exploitation and remediation—can help an organization meet the United States HIPAA legal requirements for safeguarding and protecting electronic systems where health information is accessed, stored or transmitted.

Introduction

Healthcare organizations and the information they keep are particularly vulnerable to attacks and intrusions because the correct functioning of their information systems and infrastructures is critical to the health of their patients. Grave injury and death may result from a network, computer system, or application outage, potentially caused by a security breach such as a DOS attack or an unauthorized network intrusion. Health information can be stolen for monetary or criminal purposes.

The general industry trend towards business digitization compounds the criticality of keeping hospital and health facilities' networks and systems up and running and free from intrusion. Safety and security of health applications and information is therefore paramount, and the United States' Health Insurance Portability and Accountability Act (HIPAA) law of 1996, subsequently updated and strengthened in 2013, addresses these risks from a regulatory perspective—describing administrative rules, procedures and accountability to protect the privacy and security of an individual's health information maintained in electronic health records and other formats.

Overview of HIPAA

A full description of HIPAA legal requirements is contained in the Health and Human Services (HHS) Code of Federal Regulations (CFR) 45 Public Welfare law. In short, the law contains:

- **The Privacy Rule**—Standards for Privacy of Individually Identifiable Health Information—establishes privacy rules and standards to protect individuals' health records and other personal information. The rule applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

- **The Security Rule**—Security Standards for the Protection of Electronic Protected Health Information—establishes security rules and standards for protecting health information that is accessed, stored or transferred in electronic form. The Security Rule addresses the technical and non-technical safeguards that organizations, termed "covered entities", must put in place to secure individuals' electronic Protected Health Information" (ePHI).

Covered entities—encompassing organizations that deal with patient records, including hospitals, research universities, health insurers, clinical research organizations and pharmaceutical companies—are required to have HIPAA-compliant systems to ensure the privacy of electronic health records and data (including ePHI and Electronic Medical Records, EMR) when accessed, stored or transmitted.

This paper discusses compliance with the HIPAA Security Rule to protect information when accessed, stored or transmitted electronically, and how RidgeBot's security capabilities can help your organization meet these requirements. Applicable sections of the Security Rule include:

- **Administrative Safeguards (Security Rule §164.308):** The assignment of security responsibility to an individual or team, security and access management, protection from malicious software, and security incident handling.

- **Physical Safeguards (Security Rule §164.310):** The mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion.

- **Technical Safeguards (Security Rule §164.312):** Automated processes used to protect data, control access to data—including authentication and integrity (encrypting and decrypting data as it is being stored and/or transmitted).

- **Policies, Procedures and Documentation Requirements (Security Rule §164.316):** Adoption, maintenance and documentation of appropriate policies and procedures to comply with the provisions of the Security Rule.

- **Breach Notification (Security Rule §164.402-410):** Stipulation of who, and when, to notify when a security breach has occurred.

For an organization to be HIPAA compliant, they must:

- Have processes and procedures in place to meet all the HIPAA requirements.
- Have technical security requirements covered.
- Have all processes, procedures and safeguards (technical or otherwise) documented.
- Have a person on staff responsible for HIPAA training, awareness and ensuring ongoing compliance.

HIPAA is administered and enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Compliance enforcement and verification are done primarily via self-assessment and documentation. Complaints are investigated, and HHS conducts periodic audits. Fines are levied if there is a breach or someone files a HIPAA complaint. Additional information can be found here.

Compliance with HIPAA Security Rule requirements took effect in April 2005 as given in §164.318 of the Regulation.

HIPAA Regulation Content Outline

To provide perspective on where RidgeBot can help with compliance, the structural outline of the HIPAA Regulation—CFR 45 Public Welfare—is given below, highlighting the specific sections that concern the protection of digital resources.

Most of the requirements (all except select sections of Part §164) in the regulation concern manual procedures, human accountability, workforce training and conduct, the rights of individuals regarding their health records, rules governing what health information may be shared by which organizations under what circumstances, and many other behavioral requirements of the health industry and health providers—all these requirements are independent of technology or digital resources.

The full text of the HIPAA regulation is contained in the Health and Human Services (HHS) law CFR 45, the details can be viewed here. Requirements applicable to technology and digital resources appear in Part §164, subparts C, D and E.

CFR Title 45: PUBLIC WELFARE

- **Subtitle A:** Department of Health and Human Services
  - Subchapter A: General Administration (Parts 1-102)
  - Subchapter B: Requirements Relating to Health Care Access (Parts 140-159)
  - Subchapter C: Administrative Data Standards and Related Requirements (Parts 160-169)
    - Part 160: General Administrative Requirements (§160.101-552)
      - Subpart A: General Provisions (§160.101-105)
      - Subpart B: Preemption of State Law (§160.201-205)
      - Subpart C: Compliance and Investigations (§160.300-316)
      - Subpart D: Imposition of Civil Money Penalties (§160.400-426)
      - Subpart E: Procedures for Hearings (§160.500-552)
    - Part 162: Administrative Requirements (§162.100-1902)
    - Part 163 [Reserved]
    - Part 164: Security and Privacy (§164.102-534)
      - Subpart A: General Provisions (§164.102-106)
      - Subpart B [Reserved]
      - Subpart C: Security Standards for the Protection of Electronic Protected Health Information (§164.302-318)
      - Subpart D: Notification in the Case of Breach of Unsecured Protected Health Information (§164.400-414)
      - Subpart E: Privacy of Individually Identifiable Health Information (§164.500-534)
    - Parts 165-169 [Reserved]
  - Subchapter D: Health Information Technology (Parts 170-179)
- **Subtitle B:** Regulations Relating to Public Welfare

Overview of How RidgeBot can Help

RidgeBot helps you find security deficits in your assets, and provides guidance and priority ranking on how to immediately remediate any exposures. Moreover, RidgeBot helps you maintain, on a continuing and cost-effective basis, a security posture that is always in compliance with the latest attack methods and threat intelligence.

Some of RidgeBot's key benefits to your organization's security posture include:

- **Improve and Simplify Security Activities and Process**

  o Discover, inventory and document system components, assets and attack surfaces. Because RidgeBot is fully automated, you can do this continuously, or at much more frequent intervals, than previous periodic manual processes.

  - o Reports help document vulnerabilities found, exploited, remediated and validated.
  - o Reports provide clear risk ranking to focus manual remediation activity on the highest risk vulnerabilities.
  - o RidgeBot's flexibility allows you to run attack testing from inside and outside your environment.
  - o RidgeSecurity's Threat Intelligence Platform knowledge base ensures that you are always up to date with industry-leading security vulnerability information.
  - o Run RidgeBot attacks, scans and exploitations as a standard part of your ongoing security policy.

- **Continuous Security Validation**
  - RidgeBot provides no-cost iterative, continuous hardening and asset inventory. You can run different scans and exploitations periodically or continuously—be cause it is fully automated, no manual intervention is required until a vulnerability is reported.

  - Continuous monitoring and asset discovery protect against hacker intrusion caused by an employee (or any other person) accidentally or maliciously connecting untrusted or unplanned IoT, wireless or other unauthorized devices to the environment.

  - Scan reports provide a short list of must-fix exploitable vulnerabilities to document and resolve. Report output ensures all software patches and updates needed to resolve dangerous vulnerabilities are installed on all affected assets.

- **DevOps/SecOps Software Development and Patch/Release Testing**
  - Use RidgeBot during the software development process to help ensure that dangerous coding practices that introduce vulnerabilities never ship in new releases of software.

  - Use RidgeBot to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into the production environment.

- **Security Posture Validation**
  - Continuously, iteratively attack the production environment to maintain security posture and discover misconfigurations in wireless or defensive security appliances or services such as firewall rules or UTM appliances.

  - Continuously monitor and harden login credentials on sensitive assets.

- **Compliance Audit**
  - Continuous asset discovery scanning, and attack and exploitation attempts (and the reports issued) mean your environment is always audit-ready.

  - Use RidgeBot reports to submit evidence of vulnerabilities probed, remediated and resolved.

- **Security Incident Response**
  - o Scan reports, containing recommended solutions for each vulnerability found, provide critical information to your security incident response/escalation team.
  - o Risk ranking of vulnerabilities feed into the priorities and procedures for incident response.
  - o RidgeBot AI/ML exploitation attacks provide forensic capabilities to investigate the origin and path taken by a breach, as well as step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans that you can easily use, as well as the flexibility to completely customize your own scans. The system templates include:

- **Full scan:** This test launches numerous attack techniques used by real-world hackers. Based on threat intelligence and an exploit knowledge base, RidgeBot profiles assets, mines vulnerabilities and launches attacks against target assets, which may be internal or external to your environment, in a private or public environment.

- **Ransomware scan:** This test is specifically focused on combating ransomware attacks. It launches scans for 27 high-profile ransomware entry point vulnerabilities, includes the ability to attack and exploit these vulnerabilities, and reports in detail exactly how successful exploitations were achieved. Definitions of more ransomware attacks will be added over time, and you can add these to your security arsenal by downloading periodic RidgeBot updates.

- **Weak password scan:** This test launches direct or iterative attacks based on sensitive information collected via weak credential or unauthorized access vulnerabilities. Attack targets include redis, elasticsearch, ActiveMQ, database, web login and other applications.

- **Struts2 scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using the Struts 2 framework.

- **Weblogic scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using Weblogic middleware.

- **Web scan:** This test launches cyberattacks against target websites, web applications and all related attack surfaces to gain control of the target website for both self-developed and contact management system-based websites.

- **Host scan:** This test launches direct or iterative attacks from inside a corporate network to validate the security system's response to an internal threat. Target systems include all network-accessible internal hosts and servers.

HIPAA Implementation Requirements

HIPAA Security Rule requirements applicable to technology and digital resources appear in the HIPAA Regulation Part §164, subparts C, D and E. Applicable sections of the Security Rule include:

- Administrative Safeguards: §164.308
- Physical Safeguards: §164.310
- Technical Safeguards: §164.312
- Policies, Procedures and Documentation Requirements: §164.316
- Breach Notification: §164.402-410

Requirements in the regulation are annotated with an S, R or A designation:
- **S—Standard:** A covered entity must comply with a standard.
- **R—Required:** Similar to a standard in that compliance is compulsory.
- **A—Addressable:** Covered entities must perform an assessment to determine wheth er the specification is a reasonable and appropriate safeguard in the covered entity's environment.

The specifics of the HIPAA Security Rule requirements are given in two tables in each of the sections below:

1) **Summary Table:** The columns in this table give:
   - Regulation title/category.
   - A paragraph reference to the section of the HIPAA law containing the full text of this regulation title/category.
   - List of the requirements (termed "implementation specifications" within the HIPAA l egal text) within this title/category.
   - An assessment of whether a technological solution is applicable (Yes or N/A) to complying with this requirement (some requirements are manual or procedural and cannot be complied with via technological solutions).

2) **Details Table:** For each requirement that can be satisfied with a technological solution (as per the last column of Table 1), the columns in this table give:

- A paragraph reference to the section of the HIPAA law containing the full text of this requirement.
- An extract of the text of the requirement.
- A cross-reference (right-most column) to specific RidgeBot capabilities that can be used to help you comply with the requirement—this entry cross-references the RidgeBot capabilities given in the last section of this document entitled "RidgeBot Capabilities Summary".

Administrative Safeguards (§164.308)

The HIPAA 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 health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Summary Table

Standard/Regulation	Section	Implementation Specifications (S=Standard, R=Required, A=Addressable)	Appli-cability
Security Management Process	164.308(a)(1)	(S) Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)	Yes Yes Yes N/A Yes
Assigned Security Responsibility	164.308(a)(2)	(R)	N/A
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	Yes N/A N/A
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions (R) Access Authorization (A) Access Establishment and Modification (A)	Yes N/A N/A
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	N/A Yes Yes Yes
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	Yes
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedures (A) Applications and Data Criticality Analysis (A)	N/A N/A Yes Yes N/A
Evaluation	164.308(a)(8)	(R)	Yes
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangements (R)	Yes

Details Table

Section	Regulation Implementation Specifications (S=Standard, R=Required, A=Addressable)	RidgeBot Reference
164.308(a)(1)	**Security Management Process (S):** "Implement policies and procedures to prevent, detect, contain, and correct security violations."	All
164.308(a)(1)(ii)(A)	**Risk Analysis (R):** "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."	A1-2, D1-2, R1, S1, V1, V3-5, W1
164.308(a)(1)(ii)(B)	**Risk Management (R):** "Implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level."	A3, D3, R2, S3, V1, V4-5, W1
164.308(a)(1)(ii)(D)	**Information System Activity Review (R):** "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."	A3, D1-2, R1, S3, V1, W1
164.308(a)(3)(ii)(A)	**Authorization and/or Supervision (R):** "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."	D1, S2, V3, W1-2
164.308(a)(4)(ii)(A)	**Isolating Health Care Clearinghouse Functions (R):** "If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization."	A1-2, D1, S1-3
164.308(a)(5)(ii)(B)	**Protection from Malicious Software (A):** "Procedures for guarding against, detecting, and reporting malicious software."	A1-2, D1-2, R1-2, S3, V1, V5
164.308(a)(5)(ii)(C)	**Log-in Monitoring (A):** "Procedures for monitoring log-in attempts and reporting discrepancies."	W1-2
164.308(a)(5)(ii)(D)	**Password Management (A):** "Procedures for creating, changing, and safeguarding passwords."	W1
164.308(a)(6)(ii)	**Response and Reporting (R):** "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."	A3, D2-4, R1-2, S3, V1
164.308(a)(7)(ii)(C)	**Emergency Mode Operation Plan (R):** "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."	D1, S1, S3, V1, V5

Section	Regulation Implementation Specifications (S=Standard, R=Required, A=Addressable)	RidgeBot Reference
164.308(a)(7)(ii)(D)	**Testing and Revision Procedures (A):** "Implement procedures for periodic testing and revision of contingency plans."	D2, S3, V1-5
164.308(a)(8)	**Evaluation (S):** "Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart."	D1-2
164.308(b)(1,2,3)	**Written Contract or Other Arrangements (R):** "A covered entity/business associate may permit a business associate/contractor to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate/contractor will appropriately safeguard the information."	S1

Physical Safeguards (§164.310)

The HIPAA 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."

Summary Table

Standard/Regulation	Section	Implementation Specifications (S=Standard, R=Required, A=Addressable)	Applicability
Facility Access Controls	164.310(a)	(S) Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	Yes N/A Yes Yes Yes
Workstation Use	164.310(b)	(R)	N/A
Workstation Security	164.310(c)	(R)	Yes
Device and Media Controls	164.310(d)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)	N/A N/A Yes N/A

Details Table

Section	Regulation Implementation Specifications (S=Standard, R=Required, A=Addressable)	RidgeBot Reference
164.310(a)(1)	**Facility Access Controls (S):** "Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."	A1-3, S2, V3, W2
164.310(a)(2)(ii)	**Facility Security Plan (A):** "Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."	A1-3, S2, V3, W2
164.310(a)(2)(iii)	**Access Control and Validation Procedures (A):** "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."	A1-3, S2, V3, W2
164.310(a)(2)(iv)	**Maintenance Records (A):** "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)."	A1-3, S2, V3, W2
164.310(c)	**Workstation Security (R):** "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."	D1, R1, S1, S3, V1, V5, W1
164.310(d)(2)(iii)	**Accountability (A):** ""Maintain a record of the movements of hardware and electronic media and any person responsible therefore."	A1-3, D1-2

Technical Safeguards (§164.312)

The HIPAA Security Rule defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

Standard/Regulation	Section	Implementation Specifications (S=Standard, R=Required, A=Addressable)	Appli-cability
Access Control	164.312(a)	(S) Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	Yes N/A N/A N/A N/A
Audit Controls	164.312(b)	(R)	Yes
Integrity	164.312(c)	Mechanism to Authenticate Electronic Protected Health Information (A)	Yes
Person or Entity Authentication	164.312(d)	(R)	N/A
Transmission Security	164.312(e)	Integrity Controls (A) Encryption (A)	Yes N/A
Safeguards	164.530(c)(2)	(S)	Yes
Policies and Procedures	164.530(i)(1)	(S)	Yes

Details Table

Section	Regulation Implementation Specifications (S=Standard, R=Required, A=Addressable)	RidgeBot Reference
164.312(a)(1)	**Access Control (S):** "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."	A1-2, D1-2, R1, S3, V1, V5, W1
164.312(b)	**Audit Controls (R):** "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."	A3, D1, V4, W1
164.312(c)(1)	**Mechanism to Authenticate Electronic Protected Health Information (A):** "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."	A3, D1, S3, V1, V3, V5, W1
164.312(e)(1)	**Integrity Controls (A):** "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."	S1
164.530(c)(2)	**Safeguards (S):** "(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards."	A1-2, D1, R1, S3, V1, V5, W1
164.530(i)(1)	**Policies and Procedures (S):** "A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards and implementation specifications."	All

Policies, Procedures and Documentation Requirements (§164.316)

The HIPAA Security Rule defines that covered entities must document their policies and procedures, as well as any changes to these.

Standard/Regulation	Section	Implementation Specifications (S=Standard, R=Required, A=Addressable)	Applicability
Policies and Procedures	164.316(a)	(S)	Yes
Documentation	164.316(b)	(S) Time Limit (R) Availability (R) Updates (R)	Yes N/A N/A Yes

Details Table

Section	Regulation Implementation Specifications (S=Standard, R=Required, A=Addressable)	RidgeBot Reference
164.316(a)	**Policies and Procedures (S):** "Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart."	All
164.316(b)(1)	**Documentation (S):** "(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."	A3, D1, V4, W1
164.316(b)(2)(iii)	**Updates (R):** "Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."	A2-3, D1-2

Breach Notification (§164.402-164.410)

The HIPAA Security Rule section §164.402 defines a breach to be "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [§164] which compromises the security or privacy of the protected health information".

The Breach Notification rule specifies that notification of a breach must be given to individuals (§164.404), the media (§164.406), the overseeing government secretary (§164.408) and business associates (§164.410) within given timeframes, generally within 60 calendar days from the discovery of a breach.

RidgeBot's forensic scan analysis after a security incident has taken place can help determine where and how a breach was perpetrated. From there it can be quickly extrapolated as to which systems and what data might have been exposed, assisting with critical intelligence to identify breach notification targets and meet the required notification timelines.

RidgeBot Capabilities Summary

RidgeBot Reference	Capability Description
Automated Asset Discovery and Inventory	
A1	Automated asset discovery can help you compile and maintain an **inventory** of all data processing assets and attack surfaces.
A2	An asset discovery scan iteratively **discovers and documents changes** in the presence of assets that should be included in a risk assessment or asset inventory.
A3	An automated asset discovery scan verifies on an ongoing basis that **no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities**. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
Documentation, Reporting and Forensics	
D1	Regular automated asset discovery scans on an ongoing basis can help **ensure all assets and attack surfaces are identified and documented.**
D2	Scan-and-exploitation reports can assist you in **compiling consistent and comparable documentation of vulnerabilities** found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information can be used to take mitigation actions and/or to prepare management reports.
D3	Scan-and-exploitation reports—which include recommended solutions for each vulnerability—provide critical information for your **security incident response/escalation or forensics** team to ensure timely and effective handling of all situations.
D4	A forensic scan—after a security incident has occurred—can **help determine where and how the breach was perpetrated**. From there it can be extrapolated as to which systems and what data might have been exposed.
Risk Assessment and Mitigation	
R1	A pen-test-and-exploit scan identifies, analyzes and evaluates all risks found. The scan reports provide **a ranked list of vulnerabilities found** based on each vulnerability's likelihood to be exploited, including those that were successfully exploited during the test. The reports also provide an evaluation with granular steps to remediate each vulnerability.
R2	The recommended **remedial steps in RidgeBot reports** provide evidence that risks are being adequately found, measured, reviewed and treated.
Scanning and Penetration Testing	
S1	A pen-test-and-exploit scan helps **verify the security posture of all internal systems, as well as any provider- or cloud-hosted** assets and services.
S2	A pen-test-and-exploit scan can **reveal weak points in physical security processes and systems** (cameras, surveillance systems, logging systems, digitally-controlled door locks) that could grant an attacker physical or electronic access to secure systems or areas, or allow tampering with surveillance cameras or stored logs or footage.

RidgeBot Reference	Capability Description
S3	Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your **assets are continually locked-down and that new vulnerabilities are detected immediately** after—or often before—they're introduced into your production environment.
S4	Automated pen-test-and-exploit capabilities can be run iteratively and cost-effectively to **prepare for an audit or a third-party verification** of your security posture.
Vulnerability Exploitation and Intelligence	
V1	A full scan, with exploitation turned on, **discovers, exploits and documents all vulnerabilities** found. Run this scan as a regular part of your policy/process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
V2	A full scan, with exploitation turned on, discovers, exploits and documents all vulnerabilities found. Run this scan as **a regular part of your software development and software validation processes**.
V3	A pen-test-and-exploit scan can ensure that **all systems or devices used to document events and activities are secure from software/malware vulnerabilities** where a hacker can get access to erase or alter logs, video surveillance footage, or forensic audit trail information.
V4	A pen-test-and-exploit scan can be run as a regular part of your policy/process to **harden software patches, software upgrades, new devices, and any configuration changes** before pushing them live into the production environment.
V5	RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's **industry leading knowledge base of attack techniques and intelligence**, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to **stay abreast of emerging technical vulnerabilities** in a structured and systematic way.
Weak Password and Credentials	
W1	A weak password scan run against all assets **documents and resolves login credential vulnerabilities**.
W2	A pen-test-and-exploit scan can ensure that **all systems or devices used to document events and activities are secure from weak credential** vulnerabilities where a hacker can get access to erase or alter logs, video surveillance footage, or forensic audit trail information.

Ridge Security Technology Inc.
www.ridgesecurity.ai