No. 137

CYBERSECURITY

HIPAA Security for Healthcare

Protecting electronic health information under the HIPAA Security Rule

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 137

HIPAA Security for Healthcare

Protecting electronic health information under the HIPAA Security Rule

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

HIPAA Security for Healthcare

Protecting electronic health information under the HIPAA Security Rule

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. HIPAA is a US law; this book is not affiliated with HHS. Product and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What HIPAA is 5
2 The rules 6
3 PHI and ePHI 7
4 Covered entities and business associates 8
5 Goals of the Security Rule 9
6 Structure 10
7 Required and addressable 11
8 Flexibility and scalability 12
9 NIST guidance 13

PART II · THE SAFEGUARDS

10 Risk analysis 15
11 Risk management 16
12 Finding all your ePHI 18
13 Administrative safeguards 19
14 Workforce and training 20
15 Security incidents 21
16 Contingency planning 22
17 Physical safeguards 23
18 Technical safeguards 24
19 Encryption 25
20 Policies and documentation 26

PART III · BREACHES AND ENFORCEMENT

21 What a breach is 28
22 Breach notification 29
23 Enforcement 30

FREE SAMPLE · ojayo.com

24 Recognized security practices 31
25 Business associate agreements 32
26 Threats to healthcare 33
27 Ransomware 34

PART IV · WHAT IS NEXT

28 The proposed Security Rule update 36
29 Healthcare cybersecurity performance goals 37
30 Preparing now 38
31 For small practices 39
32 Resources 40
33 AI and new technology 41
34 Common mistakes 42
35 A worked example 43
36 Careers 44
37 A HIPAA security roadmap 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

In the United States, the **Health Insurance Portability and Accountability Act** (HIPAA) requires healthcare organizations and their vendors to protect patients' health information. The **HIPAA Security Rule** focuses on **electronic protected health information** (ePHI) and requires administrative, physical and technical safeguards.

This beginner's book explains the Security Rule in plain language: who it applies to, its safeguards, required and addressable specifications, risk analysis, business associates, breach notification, enforcement, current healthcare threats and the major update HHS proposed in January 2025, which had not been finalized at the time of writing.

What this book covers

- HIPAA's rules and who must comply.
- The administrative, physical and technical safeguards.
- Risk analysis, the cornerstone of compliance.
- Business associates, breaches and enforcement.
- Ransomware, vendors and medical devices.
- The proposed Security Rule update and practical next steps.

Who this book is for

- **Practice managers, IT and security staff** in healthcare.
- **Vendors** handling health data.

FREE SAMPLE · ojayo.com

- **Students** in health IT and compliance.

How the book is organized

- **Part I — Foundations** (Chapters 1–9): HIPAA basics, the rules, PHI and ePHI, covered entities, business associates, the Security Rule's goals, structure, required and addressable, and flexibility.
- **Part II — The safeguards** (Chapters 10–20): risk analysis, finding all ePHI, risk management, the security official, workforce and training, incidents, contingency planning, physical safeguards, technical safeguards, encryption and documentation.
- **Part III — Breaches and enforcement** (Chapters 21–27): breach definition, notification, OCR enforcement, recognized security practices, business associate agreements, threats and ransomware.
- **Part IV — What is next** (Chapters 28–37): the proposed update, performance goals, preparing for it, small practices, resources, AI and new technology, mistakes, a worked example, careers and a roadmap.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in a real practice or hospital.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on the law

This book is general information, not legal advice. Consult qualified counsel and official HHS guidance. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what HIPAA is, who it applies to and how the Security Rule is structured.

FREE SAMPLE · ojayo.com

CHAPTER 1

What HIPAA is

HIPAA protects health information.

The law

HIPAA, enacted in 1996, led to national standards protecting health information. The **HITECH Act** of 2009 strengthened enforcement and extended obligations to business associates. The HHS **Office for Civil Rights** (OCR) enforces the privacy and security rules.

Why it matters

Health records are valuable to criminals, and attacks on healthcare can disrupt patient care. Protecting ePHI is both a legal duty and a patient safety issue.

KEY IDEA

Healthcare cybersecurity protects patients, not just data.

FREE SAMPLE · ojayo.com

CHAPTER 2

The rules

HIPAA has several rules.

Rule	Covers
Privacy Rule	uses and disclosures of PHI, patient rights
Security Rule	safeguards for electronic PHI
Breach Notification Rule	notifying after breaches
Enforcement Rule	investigations and penalties

Figure 2.1 The main HIPAA rules

FREE SAMPLE · ojayo.com

CHAPTER 3

PHI and ePHI

Know what is protected.

Protected health information (PHI) is individually identifiable health information held or transmitted by a covered entity or business associate, such as diagnoses, treatment records and billing details linked to a person. **ePHI** is PHI in electronic form, the focus of the Security Rule.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare (you are reading…
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

HIPAA Security for Healthcare

Enjoyed it? The full book has 53 pages and 37 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.