IBM Security

IBM

Aligning with HIPAA mandates in healthcare

How IBM can help you develop a successful plan designed to meet security and privacy requirements

Let’s get started

IBM Security

IBM

Contents

Introduction

As just about anyone dealing with the Health Insurance Portability and Accountability Act—or HIPAA—likely knows, understanding and complying with the complexities of the regulation can be challenging. And that is especially true when it comes to implementing the HIPAA Security Rule, which requires covered entities to implement reasonable and appropriate standards in order to protect the con identiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain or transmit.

IBM has been playing a significant role in helping healthcare providers, payers and life sciences organizations understand and comply with the broad set of HIPAA requirements, including the HIPAA Security Rule. We've had firsthand experience supporting organizations—of all sizes—in helping to assess their needs and meet their specific regulatory requirements.

That experience has allowed us to develop a broad portfolio of products and services designed to help address our clients' specific needs and support them in organizing their compliance teams' efforts to implement the directives of HIPAA.

Aligning with other security frameworks

Healthcare organizations may choose to employ additional security framework options in addition to those of HIPAA. For example, the National Institute of Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity in 2014, providing a risk-based approach to helping organizations in all industries understand, communicate and manage cybersecurity risks.

In the healthcare industry, where covered entities must comply with the HIPAA Security Rule, the NIST Cybersecurity Framework can offer additional support for managing compliance.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find they've developed a strong basis for assessing risk, measuring compliance and identifying potential gaps in their programs. And addressing these gaps can bolster their compliance with the HIPAA Security Rule and improve their ability to secure ePHI and other critical information and business processes.

But it's important to note that healthcare organizations shouldn't assume that they're in compliance with the HIPAA Security Rule—even if they've aligned their security program to the NIST Cybersecurity Framework. Similarly, while it may be relevant to certain controls, the HIPAA Security Rule does not require covered entities to integrate the NIST Cybersecurity Framework into their security management programs. Covered entities and business associates should perform their own security risk assessments to identify potential gaps and mitigate ePHI threats to their systems.

Three types of prescribed safeguards

HIPAA clearly identifies requirements for three types of safeguards for entities covered by ePHI regulations.

1. **Administrative safeguards**
   HIPAA administrative safeguards require documented policies and procedures for day-to-day operations when handling PHI, managing employee conduct as it relates to PHI and managing the selection, development and use of security and privacy controls. For instance, administrative safeguards require written procedures that cover access to PHI and associated controls, audit controls and data integrity controls.

2. **Physical safeguards**
   HIPAA physical safeguards comprise a series of security measures designed to protect the environment in which systems containing ePHI reside—including buildings and equipment—from natural and environmental hazards, as well as unauthorized intrusion. Physical safeguards include access controls, workstation controls, and data and media controls.

3. **Technical safeguards**
   The technical safeguards mandated by HIPAA include security measures that specify how to use technology to protect and control access to ePHI. For example, technical safeguards lay out requirements for workforce security and information access.

How IBM can help build and support your security framework

IBM® Security solutions offer a broad portfolio that can help you address the HIPAA Security Rule requirements—and help you to incorporate the NIST framework and other frameworks. In doing so, we can help you meet your more comprehensive HIPAA compliance goals and objectives of enhancing cost efficiency and simplifying management to help you avoid perceived gaps in coverage as threats evolve and change.

For organizations with more mature security strategies and more complex and demanding protection needs, IBM Security solutions provide a broad set of controls and integrated actions designed to support various risk profiles.

An overview of HIPAA-related IBM solutions

	Administration									Physical				Technical				
Security categories	Security management process 164.308 (a) (1)	Assigned security responsibility 164.308 (a) (2)	Worforce security 164.308 (a) (3)	Information access management 164.308 (a) (4)	Security awareness and 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)	Facillity access controls 164.310 (a)	Workstation use 164.310 (b)	Workstation security 164.310 (c)	Device and media 164.310 (d)	Access control 164.312 (a)	Audit control 164.312 (b)	Integrity 164.312 (c)	Person or Entity Authorization 164.312 (d)	Transmission Security 164.312 (e)
Security intelligence	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■
Advanced fraud protection					■													
Identity and access management	■		■	■	■					■				■	■		■	■
Data secuirity	■		■	■	■	■	■							■	■	■	■	■
Infrastructure security (mobile, network, endpoint, mainframe)	■		■	■	■	■					■	■	■	■			■	■
Application security	■		■	■	■													
Intelligence analysis (i2)	■		■		■	■	■			■								
Security services	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■		■

This is a summary showing where IBM offers solutions related to specific HIPAA standards. For a more detailed listing, please see the appendix.

Why IBM

HIPAA can present healthcare organizations with several challenges where information security is concerned. And while the HIPAA Security Rule requirements offer covered entities considerable flexibility regarding the ways in which to meet requirements, it can be challenging to determine which path to compliance is the optimal one to take for your organization.

IBM offers a broad set of solutions and services designed to help your organization develop and implement the more comprehensive HIPAA security compliance strategies your organization needs to reach its goals. Within that context, we deliver leading technology and an experienced practice, intended to consider your unique account situation.

When you collaborate with IBM, you gain access to a security team of 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. And with an approach that includes advanced cognitive computing, we enable organizations like yours to continue to innovate while mitigating risk. So you can continue to grow your business—while using processes designed to secure your most critical data and processes.

For more information

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

Additionally, IBM Global Financing offers numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition.
For more information, visit:
ibm.com/financing

IBM Security solutions may be used to help align to a HIPAA regulatory environment

Category	Full product name	Short name/abbreviation	Short description
Security Intelligence	IBM QRadar® Advisor with Watson	IBM QRadar Advisor with Watson	Combines the cognitive capabilities of Watson and QRadar Security Analytics Platform to uncover hidden threats and automate insights
	IBM Security QRadar Incident Forensics	QRIF	Reduce time to investigate incidents, and remediate more thoroughly
	IBM Security QRadar Log Manager	QRadar LM	Turn-key log management, SMB to enterprise (upgradeable to SIEM)
	IBM Security QRadar QFlow Collector	Qflow	Layer 7 application monitoring of physical network traffic (includes VFlow)
	IBM Security QRadar Network Insights	QNI	Enables attack prediction through real-time network traffic analysis
	IBM Security QRadar SIEM	QRadar SIEM	Security intelligence & IBM Sense Analytics, protecting assets & information from advanced threats
	IBM QRadar on Cloud	QRoC	Outsources security intelligence deployment/support, by offering QRadar as a service
	IBM QRadar User Behavior Analytics	QRadar UBA	An app that provides early visibility to insider threats
	IBM Security QRadar Vulnerability Manager	QVRM	Intelligent scanning - identifies and prioritizes vulnerabilities – integrates for prioritization insights
	i2® Intelligence Analysis Platform (including i2 Enterprise Insight Analysis and i2 Analyst's Notebook)	i2	A system that facilitates the analysis, production, and reporting of security intelligence
	Resilient® Incident Response Platform	Resilient IRP	Allows security teams to easily configure incident response plans/technologies
Advanced Fraud Protection	IBM Security Trusteer® Fraud Protection Suite	Fraud Protection Suite	Designed to detect, enforce, investigate and remediate fraud fast and efficiently
	IBM Security Trusteer Pinpoint Detect	Pinpoint Detect	Real-time detection of Man-in-the-Browser malware infected devices
	IBM Security Trusteer Pinpoint Malware Detection	Pinpoint Malware Detection	Designed to provide conclusive detection of criminals and account takeover attempts
	IBM Security Trusteer Rapport	Rapport	Client-based endpoint detection, mitigation/remediation against financial malware/ phishing attacks
	IBM Security Trusteer Rapport for Mitigation	Rapport for Mitigation	Mitigation/remediation against financial malware
	IBM Security Trusteer Mobile SDK	Mobile SDK	Android/iOS library for native mobile apps detect compromised/vulnerable devices
	IBM Security Trusteer Mobile Browser	Mobile Browser	Secure mobile browser for safe web access
Identity and Access Management (People)	IBM Security Access Manager for ESSO	SAM ESSO	SSO, password management, session management, compliance and user productivity gains
	IBM Security Access Manager	SAM	All-in-one access appliance for web, mobile and cloud
	IBM Security Access Manager for DataPower	SAM for DataPower	Web access management software module for IBM DataPower Gateways
	IBM Cloud Identity Connect	CIC	Securely connect employees to cloud services
	IBM Cloud Identity Service	CIS	Multitenant identity and access management service offered from the public cloud
	IBM Security Identity and Access Assurance	IAA or SIAA	Discounted bundle - SAM, IGI Lifecycle, Directory Suite, QRadar Log Manager
	IBM Security Identity and Access Manager	SIAM	Discounted bundle - SAM base appliance and IGI Lifecycle
	IBM Security Identity Governance and Intelligence	IGI	Govern access and evaluate regulatory compliance – bring IT and LoBs together
	IBM Security Identity Manager	SIM	Creates, modifies and terminates user privileges throughout users' lifecycles
	IBM Security Privileged Identity Manager	PIM	Keeps admin (privileged user) ID usage tracked and under control
	IBM Security Directory Suite	SDS	Real-time, event-driven, general-purpose data integration environment (includes Directory Server)

Return to How IBM can help

Next page

Category	Full product name	Short name/abbreviation	Short description
Data Security	IBM Guardium® Activity Monitor for Databases	Guardium DAM	Real time data activity monitoring with blocking/masking capabilities
	IBM Guardium Activity Monitor for Files	Guardium FAM	Discover/track/control sensitive file access (local/networked file systems)
	IBM Guardium Vulnerability Assessment	Guardium VA	Vulnerability assessment for databases
	IBM Guardium Data Encryption	Guardium DES	DBMS encryption (Oracle, SQL Server, DB2, IMS, …) and file encryption
	IBM Guardium Data Encryption for DB2 and IMS Databases	Guardium DES for z/OS	Data encryption for both DB2 and IMS databases on z/OS
	IBM Guardium Data Redaction	Guardium Data Redaction	Designed to protect sensitive data in documents and forms from unintentional disclosure
	IBM Multi-Cloud Data Encryption	MDE	Designed to protect databases, file shares, data warehouses, and big data implementations in private/hybrid/public clouds
	IBM Multi-Cloud Data Protection	Multi-Cloud Data Protection	Designed to safeguard critical data where it resides, with cloud-based capabilities
	Agile® 3 GRC Command & Control Center	Agile 3	A dashboard designed to provide visibility to identify potential risks to sensitive assets
	IBM Security Key Lifecycle Manager	RSKLM	Enterprise management of encryption keys (key server on distributed platforms)
	IBM Security Key Lifecycle Manager for z/OS	SKLM for z/OS	Enterprise management of encryption keys (key server on mainframe)
	IBM Key Protect	Key Protect	Manages the lifecycle of encryption keys for apps across Bluemix®
Application Security	IBM Application Security on Cloud	ASoC	Provides static, dynamic and interactive application security testing on cloud apps
	IBM Security AppScan® Enterprise	AppScan Enterprise	Enterprise dynamic (unattended, parallel) app scanning and reporting
	IBM Security AppScan Source	AppScan Source	Static testing of application source code for vulnerabilities
	IBM Security AppScan Standard	AppScan Standard	Dynamic testing of running web applications for vulnerabilities
Infrastructure Security (Mobile, Network, Server and Endpoint)	IBM MaaS360®	MaaS360	Enterprise mobile platform - security/management for applications/documents/devices
	IBM X-Force® Exchange Commercial API	X-Force Exchange Comm API	API that makes a wide range of IBM Security Threat Intelligence available
	IBM BigFix® Compliance	BigFix Compliance	Designed to protect endpoints. Better meet security compliance. Designed to reduce costs and enhance agility
	IBM BigFix Patch	BigFix Patch	Server management – lifecycle management; security and compliance and server automation
	IBM BigFix Inventory	BigFix Inventory	Software asset management – designed to discover all licensed/unlicensed software for all devices
	IBM BigFix Detect	BigFix Detect	Integrates attack detection with remediation capabilities for endpoint security
	IBM BigFix Lifecycle	BigFix Lifecycle	Find/fix endpoint problems - connected or not, fixed or mobile, virtual or physical
	IBM Security zSecure® Admin	zSecure Admin	Solution to improve administration, audit, and compliance for System z
	IBM Security zSecure Audit	zSecure Audit	Provides highly customizable reporting and analysis of audit records
	IBM Security zSecure Alert	zSecure Alert	Real-time threat monitoring extending RACF/ACF2 real-time notification capabilities
	IBM Security zSecure Command Verifier	zSecure CV	Designed to control compliance – by preventing erroneous or out-of-policy RACF commands
Security Services	Security Strategy, Risk and Compliance	SSRC	Assess, evaluate, and recommend to improve security risk management
	Security Intelligence and Operations Consulting	SIOC	Advise for the development of intelligence-driven security operations
	Infrastructure and Endpoint Security	IES	Managed security services for network, web, and messaging security
	Data and Application Security	DAS	Consulting and managed services for data security, including encryption
	X-Force Red Offensive Security	XFP	Security testing program focused on vulnerability management, rapid testing, and analytics
	X-Force Incident Response and Intelligence Services	XF IRIS	Prepare clients to respond to threats and incidents across the entire incident lifecycle
	Identity and Access Management	IAM	Consulting services recommending and integrating IAM components
	IT Risk Management Services	ITRMS	Create an IAM strategy and assist in deploying appropriate IAM solutions

Return to How IBM can help

Legal

IBM Security

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
September 2017

WGB03046-USEN-02