FEBRUARY 2024

HIPAA SECURITY COMPLIANCE

Becoming HIPAA Compliant with MedStack

MEDSTACK®

CONTENTS

INTRODUCTION

As the adoption of digital healthcare tools and technologies continues to progress, healthcare organizations have become increasingly more susceptible to cyberattacks. Balancing the need for security and privacy protection with the need to deliver improved outcomes is extremely complex, particularly as cloud-based systems allow authorized parties to access electronic information with minimal effort.

Scope

The Health Insurance Portability and Accountability Act (HIPAA) mandates that healthcare organizations ensure the security of their systems and the confidentiality of patient data. This paper provides an outlook on HIPAA compliance, and will evaluate how organizations are able to reduce their security liabilities and uphold a HIPAA compliant stance.

Examples of MedStack's solutions that are relevant to the HIPAA Security Rule will also be explored within the context of NIST Special Publication 800-66. Finally, this paper will evaluate the substantial benefit that MedStack's solutions are able to provide so that organizations can more easily maintain compliance with HIPAA.

Definitions

- "Business Associate" has the same meaning as the term "business associate" at 45 CFR 160.103.
- "Covered Entity" has the same meaning as the term "covered entity" at 45 CFR 160.103.
- "HIPAA" means the Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations.
- "HIPAA Security Rule" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- "NIST" means National Institute of Standards and Technology, who provide measurable solutions and promote equitable standards.
- "PHI" means "protected health information" as defined in 45 CFR 160.103 that is received by MedStack from or on behalf of you.
- "ePHI" means PHI that is stored and shared electronically.
- "OCR" means the "HHS' Office for Civil Rights," an organization that is responsible for issuing annual guidance on the provisions, and is responsible for enforcing HIPAA Security Rules.

HIPAA OVERVIEW

Who Needs to Be HIPAA Compliant?

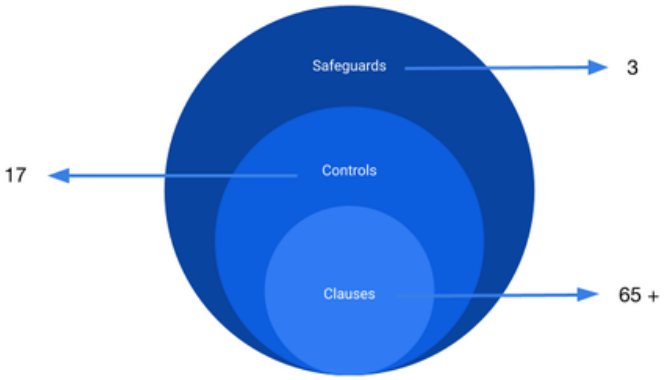
Covered Entities (any entity that offers treatment, payment processing, or operational services in a healthcare setting) and Business Associates (entities that have access to PHI and support the above-mentioned activities) must be HIPAA compliant.

All healthcare organizations operating in the US need to be HIPAA compliant. Organizations based outside of the US, but who use or hold patient data of US citizens, also need to be HIPAA compliant.

Safeguard Surface Area

HIPAA has 3 safeguards, 17 controls, and 65+ clauses. 25 of those clauses are required. This often amounts to organizations creating 50+ policies as they look to incorporate safeguards.

HIPAA Controls



Safeguard Themes

Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts

Technical Safeguards

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

RISK REDUCTION

HIPAA compliance reduces risk by helping organizations to establish policies and procedures for collecting, using, securing, and sharing PHI.

Becoming and remaining HIPAA compliant is a challenge for many organizations.

1. There are technical, administrative, and physical criteria that must be met. Security measures must be implemented and policies and procedures developed to ensure consistent management of these criteria.
2. When regulations surrounding HIPAA are updated, organizations must stay up to date with any new requirements and have processes to implement changes quickly to reduce risk.
3. Organizations must follow the breach notification protocols outlined by HIPAA Security Rules.
4. All personnel must be appropriately trained to be HIPAA compliant.

Fines can be enforced by the OCR upon individuals and organizations who do not comply with HIPAA Security Rules. These disciplinary actions – involving significant monetary penalties – are meant to deter inappropriate handling of PHI.

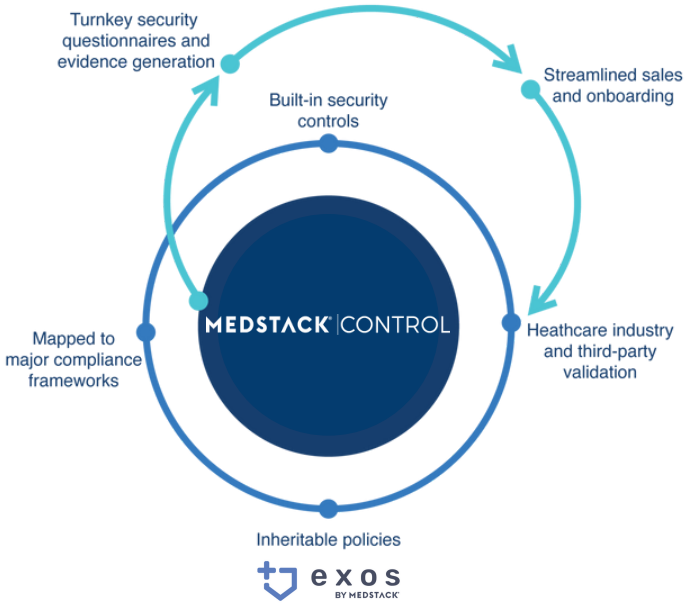
The OCR receives and investigates complaints from individuals and organizations that are potentially violating HIPAA Security Rules. Should a breach be discovered, resulting in a potential HIPAA violation, state attorneys general may authorize further sanctions and issue fines, under applicable state laws.

In most cases, when Covered Entities and their Business Associates agree that they have not complied with HIPAA Security Rules, a settlement is agreed upon and the case is resolved without admitting any wrong-doing. As part of the settlement, those involved must create an action plan to improve how they intend to follow HIPAA Security Rules.

SOLUTIONS

The Fastest Path to 100% HIPAA Compliance

Exos by MedStack combined with MedStack Control delivers a top-to-bottom healthcare data privacy compliance solution like no other.



Exos by MedStack
Establish your healthcare compliance program with training and templates. Exos by MedStack is the only compliance and risk management solution built exclusively for healthcare. Accelerate the delivery of trusted, enterprise-ready solutions to market with customizable policy and procedure templates, documented workflows, employee video training, and more.

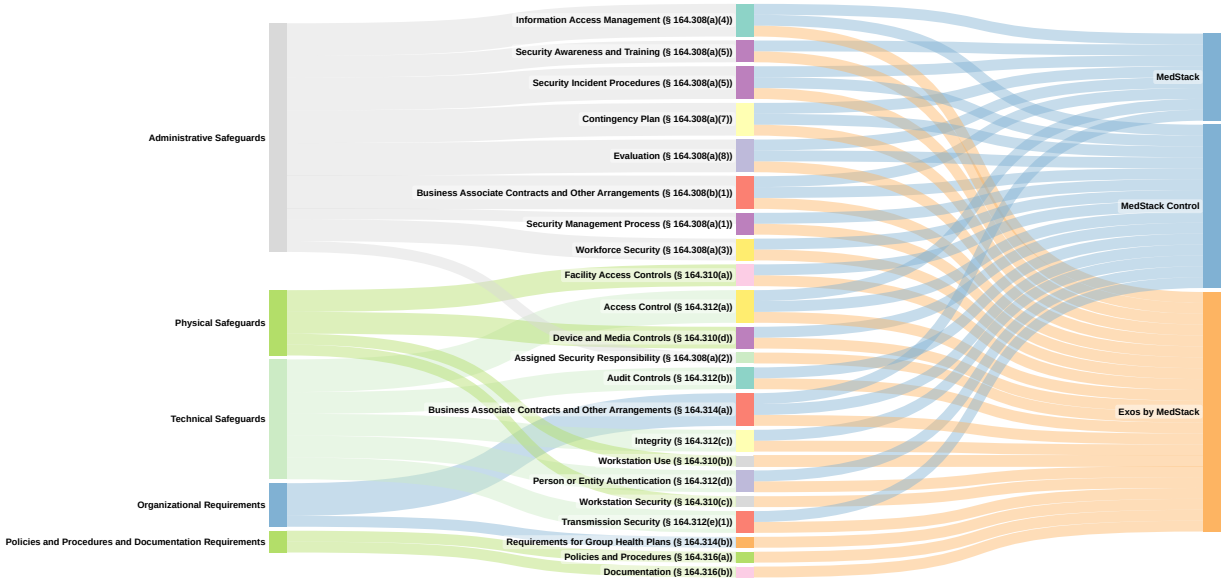
MedStack Control
Build, deploy, and maintain compliant digital health applications. MedStack Control ensures the highest level of privacy and security standards, validated by the healthcare industry. Easily deploy Amazon AWS or Microsoft Azure cloud resources with a single click using MedStack Control while ensuring your cloud services meet the HIPAA Security Rules.

Where MedStack and HIPAA Compliance Connect

The following matrix focuses on MedStack's relevance to the Physical, Technical, and Administrative domains as found in the Security Rules Standards and Implementation Specifications.

- **HIPAA Security Rule** – The HIPAA Security Rule column of the table identifies the applicable HIPAA Security Rule standard, and is organized to initiate the thought process for regulated entities to implement the requirements of the Security Rule.
- **Key Activities** – The Key Activities column of the table identifies the actions commonly linked to the security functions of the respective HIPAA Security Rule standards. Descriptions of activities that are also implementation specifications have been indicated as such, while also noting if the implementation specification is either required or addressable.
- **The MedStack Solution for HIPAA Compliance Coverage** – The final column outlines how organizations can reduce their security liabilities and uphold a HIPAA compliant stance by adopting MedStack's solutions.

This is not a prescriptive table and should not be considered comprehensive for all considerations when implementing the HIPAA Security Rule. There may be extra tasks an organization might have to think about related to how it runs that are not mentioned in the table.



HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Administrative Safeguards		
Security Management Process (§ 164.308(a)(1))	• Identify all ePHI and relevant Information Systems • Conduct Risk Assessment • Implement a Risk Management Program • Acquire IT Systems and Services • Create and Deploy Policies and Procedures • Develop and Implement a Sanction Policy • Develop and Deploy the Information System Activity Review Process • Develop Appropriate Standard Operating Procedures • Implement the Information System Activity Review and Audit Process	**Exos by MedStack** provides: • An entire Governance, Risk, and Compliance (GRC) platform that governs and guides you • Administrative policy templates for HIPAA • HIPAA Compliance Policy • A Software Inventory that contains fields to document systems and data types, including ePHI • A Physical Assets inventory to keep track of assigned employee assets • Risk Management Process Policy • Sanctions Policy • Risks module for your Risk Management Program to document human, natural, and environmental threats • Extensive auditing capabilities • Customizable procedures for turning tasks into Standard Operating Procedures • Third-party vendor agreement storage for HIPAA Business Associate Agreement (BAA) to document vendor and/or consultant access to ePHI and their obligations

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Security Management Process (§ 164.308(a)(1))	• Identify all ePHI and relevant Information Systems • Conduct Risk Assessment • Implement a Risk Management Program • Acquire IT Systems and Services • Create and Deploy Policies and Procedures • Develop and Implement a Sanction Policy • Develop and Deploy the Information System Activity Review Process • Develop Appropriate Standard Operating Procedures • Implement the Information System Activity Review and Audit Process	**MedStack Control** provides: • Default security and benchmarks for securing ePHI • Risk mitigation through third-party audited and proven controls • Extensive auditing capabilities
Assigned Security Responsibility (§ 164.308(a)(2))	• Select a Security Official to be Assigned Responsibility for HIPAA Security • Assign and Document the Individual's Responsibility	**Exos by MedStack** provides: • Policies and procedures for hiring and assigning a Security Officer • A predefined Security Officer role • Security Officer responsibilities outlined in Privacy Officer Policy and procedures

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Workforce Security (§ 164.308(a)(3))	• Implement Policies and Procedures for Authorization and/or Supervision • Establish Clear Job Descriptions and Responsibilities • Establish Criteria and Procedures for Hiring and Assigning Tasks • Establish a Workforce Clearance Procedure • Establish Termination Procedures	**Exos by MedStack** provides: • Assign Security Responsibility Policy • Privacy Officer Policy • Sanctions Policy • Security Incident Policy • A clear method to assign Tasks • Task verification strategies • Granular user permissions • Extensive auditing and enforcement capabilities through policies and procedures • Two-factor authentication (2FA) **MedStack Control** provides: • Enforced two-factor authentication (2FA) on all accounts
Information Access Management (§ 164.308(a)(4))	• Isolate Healthcare Clearinghouse Functions • Implement Policies and Procedures for Authoring Access • Implement Policies and Procedures for Access Establishment and Modification • Evaluate Existing Security Measures Related to Access Controls	**MedStack** provides: • A Standard Operating Procedure for account lockouts that rely on KYC processes to help prevent customer fraud and account takeovers • A dedicated 24/7 SOC team for incident response

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Information Access Management (§ 164.308(a)(4))	• Isolate Healthcare Clearinghouse Functions • Implement Policies and Procedures for Authoring Access • Implement Policies and Procedures for Access Establishment and Modification • Evaluate Existing Security Measures Related to Access Controls	**Exos by MedStack** provides: • HIPAA security and awareness training • Application Security & Software Development Policy • Information System Activity Review Policy • Evaluation Policy • Person or Entity Authentication Policy • Unique User Identification Policy • Granular user permissions • Extensive auditing and enforcement capabilities through policies and procedures **MedStack Control** provides: • Accurate logging and monitoring • Auditable activity log • Isolated environments

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Security Awareness and Training (§ 164.308(a)(5))	• Conduct a Training Needs Assessment • Develop and Approve a Training Strategy and a Plan • Protection from Malicious Software, Login Monitoring, and Password Management (addressable) • Develop Appropriate Awareness and Training Content, Materials, and Methods • Implement the Training • Implement Security Reminders • Monitor and Evaluate Training Plan	**MedStack** provides: • Employees trained for the safeguarding of ePHI as part of infrastructure safeguards **Exos by MedStack** provides: • HIPAA security and awareness training, as it is essential for organizations using MedStack to continue this education • HIPAA training roles and responsibilities
Security Incident Procedures (§ 164.308(a)(5))	• Determine Goals of Incident Response • Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism • Develop and Implement Policy and Procedures to Respond to and Report Security Incidents (required) • Incorporate Post-Incident Analysis into Updates and Revisions	**MedStack** provides: • Monitored SIEM • Commitment to our HIPAA Business Associate Agreement • Security Incident procedures • Breach Notification procedures • A dedicated 24/7 SOC team for incident response

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Security Incident Procedures (§ 164.308(a)(5))	• Determine Goals of Incident Response • Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism • Develop and Implement Policy and Procedures to Respond to and Report Security Incidents (required) • Incorporate Post-Incident Analysis into Updates and Revisions	**Exos by MedStack** provides: • Security Incident Policy • Breach Notification Policy • Incident feature to Respond to and Report Security Incidents **MedStack Control** provides: • 24/7 SOC monitoring and customer notification • Self-service maintenance tools
Contingency Plan (§ 164.308(a)(7))	• Develop Contingency Planning Policy • Conduct an Applications and Data Criticality Analysis (addressable) • Identify Preventative Measures • Develop Recovery Strategy • Data Backup Plan and Disaster Recovery Plan (required) • Develop and Implement an Emergency Mode Operation Plan (required) • Testing and Revision Procedure (addressable)	**MedStack** provides: • Continuity of operational systems during adverse situations • System restoration procedures in order of system criticality • Alternative data centers and geographic regions as appropriate • A dedicated 24/7 SOC team for incident response **Exos by MedStack** provides: • Disaster Recovery & Contingency Plan Policy • Emergency Mode Operations Plan Policy

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Contingency Plan (§ 164.308(a)(7))	• Develop Contingency Planning Policy • Conduct an Applications and Data Criticality Analysis (addressable) • Identify Preventative Measures • Develop Recovery Strategy • Data Backup Plan and Disaster Recovery Plan (required) • Develop and Implement an Emergency Mode Operation Plan (required) • Testing and Revision Procedure (addressable)	**MedStack Control** provides: • Self-service maintenance tools • Immutable backups • Alternative data centers and geographic regions as appropriate
Evaluation (§ 164.308(a)(8))	• Determine Whether Internal or External Evaluation is Most Appropriate • Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule • Conduct Evaluation • Document Results • Repeat Evaluations Periodically	**MedStack** provides: • Third-party verification, including, but not limited to: SOC 2 Type 2 Report, security assessments, Privacy Impact Assessments (PIA), and Threat Risk Assessments (TRA) • A customer Service Level Agreement (SLA)

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Evaluation (§ 164.308(a)(8))	• Determine Whether Internal or External Evaluation is Most Appropriate • Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule • Conduct Evaluation • Document Results • Repeat Evaluations Periodically	**Exos by MedStack** provides: • Evaluation Policy • Evaluation for Effectiveness of Security Policies and Procedures • Creation of custom policies and procedures to facilitate evidence generation for further Evaluation **MedStack Control** provides: • Ability to answer vendor security questionnaires • Secure baseline standards to evaluate against • Third-party verified SOC 2 Type 2 Trust Services Criteria for Security, Confidentiality, Availability
Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))	• Identify Entities that are Business Associates Under the HIPAA Security Rule • Establish a Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met • Written Contract or Other Arrangement (required)	**MedStack** provides: • A standardized MedStack HIPAA Business Associate Agreement that we enact with all customers **Exos by Medstack** provides: • Storage of Vendor Agreements and HIPAA Business Associate Agreements through Evidence management

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))	• Identify Entities that are Business Associates Under the HIPAA Security Rule • Establish a Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met • Written Contract or Other Arrangement (required)	**MedStack Control** provides: • Adherence to MedStack's HIPAA Business Associate Agreement
Physical Safeguards		
Facility Access Controls (§ 164.310(a))	• Conduct an Analysis of Existing Physical Security Vulnerabilities • Identify Corrective Measures • Develop a Facility Security Plan (addressable) • Develop Access Control and Validation Procedures (addressable) • Establish Contingency Operation Procedures (addressable) • Maintain Maintenance Records (addressable)	MedStack does not have physical facilities. **Exos by MedStack** provides: • Audit Control Policy • Unique User Identification Policy • Disaster Recovery & Contingency Plan Policy • Evaluation Policy • Audit Control Procedure • Emergency Access Policy • Emergency Access Procedure • Emergency Mode Operations Plan • Maintain Audit Logs and Access Reports Procedure

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Facility Access Controls (§ 164.310(a))	• Conduct an Analysis of Existing Physical Security Vulnerabilities • Identify Corrective Measures • Develop a Facility Security Plan (addressable) • Develop Access Control and Validation Procedures (addressable) • Establish Contingency Operation Procedures (addressable) • Maintain Maintenance Records (addressable)	**MedStack Control** provides: • Physical safeguards inherited by cloud providers
Workstation Use (§ 164.310(b))	• Identify Workstation and Device Types and Functions or Uses • Identify the Expected Performance of Each Type of Workstation and Device • Analyze Physical Surroundings for Physical Attributes	**Exos by MedStack** provides: • Workstation Acceptable Use Policy • Physical Assets inventory tracking

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Workstation Security (§ 164.310(c))	• Identify All Methods of Physical Access to Workstations and Devices • Analyze the Risk Associated with Each Type of Access • Identify and Implement Physical Safeguards for Workstations and Devices	**Exos by MedStack** provides: • Workstation Security Policy • Physical Assets inventory • Risk management
Device and Media Controls (§ 164.310(d))	• Implement Methods for the Final Disposal of ePHI (required) • Develop and Implement Procedures for the Reuse of Electronic Media (required) • Maintain Accountability for Hardware and Electronic Media (addressable) • Develop Data Backup and Storage Procedures (addressable)	**Exos by MedStack** provides: • Media Disposal Policy • Media Reuse Policy • Data Backup & Storage Policy **MedStack Control** provides: • Disposal of ePHI according to NIST 800-88 Guidelines for Media Sanitization by our cloud providers • Confirmation of Infrastructure Deletion (CoID) as a Standard Operating Procedure at MedStack for customer offboarding to ensure ePHI does not accidentally fall into malicious hands • Resources and accounts that are not reused for customers • Comprehensive ePHI data backup and storage

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Technical Safeguards		
Access Control (§ 164.312(a))	• Analyze Workloads and Operations to Identify the Access Needs of All Users • Identify Technical Access Control Capabilities • Ensure that All System Users Have Been Assigned a Unique Identifier (required) • Develop Access Control Policy and Procedures • Implement Access Control Procedures Using Selected Hardware and Software • Review and Update Access for Users and Processes • Establish an Emergency Access Procedure (required) • Automatic Logoff and Encryption and Decryption (addressable) • Terminate Access if it is No Longer Required	**MedStack** provides: • A Standard Operating Procedure for account lockouts that rely on KYC processes to help prevent customer fraud and account takeovers **Exos by MedStack** provides: • Unique User Identification Policy • Emergency Access Policy • Automatic logoff after inactivity • Two-factor authentication (2FA) • Encryption of data at rest **MedStack Control** provides: • Enforced two-factor authentication (2FA) on all accounts • Automatic logoff after inactivity • Encryption of data at rest

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Audit Controls (§ 164.312(b))	• Determine the Activities that Will Be Tracked or Audited • Select the Tools that Will Be Deployed for Auditing and System Activity Reviews • Develop and Deploy the Information System Activity Review/Audit Policy • Develop Appropriate Standard Operating Procedures • Implement the Audit/System Activity Review Process	**Exos by MedStack** provides: • Activity Audit log that can be downloaded as a CSV • Background Operations Audit log • Notifications for users about key policy updates and changes • Task verification strategies **MedStack Control** provides: • Activity logging at the control plane level so you know who did what and when to your infrastructure • Background File Integrity Monitoring (FIM) and Host Intrusion Detection (HID) that is trained on HIPAA Security Rules with a Standard Operating Procedure for notifying customers of suspicious activity

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Integrity (§ 164.312(c))	• 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 the Integrity Policy and Requirements • Implement Procedures to Address These Requirements • Implement a Mechanism to Authenticate ePHI (addressable) • Establish a Monitoring Process to Assess How the Implemented Process is Working	**Exos by MedStack** provides: • Person or Entity Authentication Policy • Application Security & Software Development Policy • Task verification strategies • Two-factor authentication (2FA) **MedStack Control** provides: • File Integrity Monitoring (FIM) • Activity logging at the control plane level so you know who did what and when to your infrastructure • Enforced two-factor authentication (2FA) on all accounts
Person or Entity Authentication (§ 164.312(d))	• Determine Authentication Applicability to Current Systems/Applications • Evaluate Available Authentication Options • Select and Implement Authentication Options	**Exos by MedStack** provides: • Person or Entity Authentication Policy • Custom roles and permissions within the application • Task verification strategies • Two-factor authentication (2FA) **MedStack Control** provides: • Enforced two-factor authentication (2FA) on all accounts

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Transmission Security (§ 164.312(e)(1))	• Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information • Develop and Implement Transmission Security Policy and Procedures • Implement Integrity Controls (addressable) • Implement Encryption (addressable)	**Exos by MedStack** provides: • Application Security & Software Development Policy **MedStack Control** provides: • Network-based Application Firewalls • DDoS protection • IP spoofing protection • Host-based Application Firewalls • Intrusion Detection System (IDS) monitoring • Encryption of data in transit • Encryption of data at rest • Managed load balancer

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Organizational Requirements		
Business Associate Contracts and Other Arrangements (§ 164.314(a))	• Business Associates Will Comply with the Applicable Requirements of the Security Rule (required) • Contract Must Provide that the Business Associates Enter into Contracts with Subcontractors to Ensure the Protection of ePHI (required) • Contract Must Provide that Business Associates will Report Security Incidents (required) • Other Arrangements (required) • Business Associate Contracts with Subcontractors (required)	**MedStack** provides: • MedStack HIPAA Business Associate Agreement (BAA) **Exos by MedStack** provides: • Business Associate Policy • Procedure for Privacy Officer's Responsibility for Business Associate Relation • Procedure for Business Associate Agreement • Storage of third-party vendor agreements to be used as evidence **MedStack Control** provides: • HIPAA compliance through technical safeguards • Reporting of Use or Disclosure of PHI not permitted or required by the MedStack HIPAA BAA

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Requirements for Group Health Plans (§ 164.314(b))	• Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of ePHI (required) • Amend Plan Documents of Group Health Plan to Address Adequate Separation (required) • Amend Plan Documents of Group Health Plan to Address Security of ePHI Supplied to Plan Sponsors' Agents and Subcontractors (required) • Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents (required)	Exos by MedStack does not outline specifics for Group Health Plans, as they could operate under a Health Maintenance Organization model (HMO), or Preferred Provider Organization model (PPO). Group Health Plans have the same baseline requirements for ensuring the privacy and security of PHI: • Appointing a Security Officer • PHI Uses and Disclosure Policy (HIPAA-compliant Privacy Policies) • Administrative, Physical, and Technical safeguard policies to ensure the integrity of ePHI • Breach Notification Policy • HIPAA Employee Training • Business Associate Agreements

HIPAA Security Rule	NIST Special Publication 800-66 Key Activities	MedStack Solution for HIPAA Compliance Coverage
Policies and Procedures and Documentation Requirements		
Policies and Procedures (§ 164.316(a))	• Create and Deploy Policies and Procedures • Update the Documentation of Policy and Procedures	**Exos by MedStack** provides: • Pre-defined policies and procedures • A cohesive location for all of your Update Documentation • User Notifications for policy changes
Documentation (§ 164.316(b))	• Draft, Maintain, and Update Required Documentation • Retain Documentation for at Least Six Years (required) • Ensure that Documentation is Available to Those Responsible for Implementation (required) • Update Documentation as Required (required)	**Exos by MedStack** provides: • A secure location for the HIPAA Document Privacy Rule of six years • Pre-defined policies and procedures for safeguarding and securing PHI • Policy and procedure assignment to ensure Documentation is Available to Those Responsible for Implementation • Policy drafts, histories, and versioning • An auditable log of policy changes

WHY MEDSTACK

MedStack is the only solution that combines built-in policy templates and procedure workflows with the power of fully managed security controls, so you can automatically provide the assurance needed to sell your application. Healthcare organizations around the world trust MedStack to deliver the highest level of healthcare data security and privacy.

Built for Digital Health

MedStack's security posture has been reviewed and accepted in implementation by healthcare enterprises, government agencies and academic institutions, including several notable payers and providers in North America.

HIPAA Compliant by Design

Privacy and security compliance is proactively built-in and hard-coded into MedStack's platform, not just delivered as a task list that then requires implementation.

All-In-One Solution

With an exclusive focus on data security and privacy for digital health, MedStack brings together a turnkey cloud developer experience with industry-proven security architecture, inheritable policies, evidence generation tools for certifications, and a seamless system for aligning validated responses to vendor security assessment questionnaires.

Hospital and Health System Innovation

One problem with developing a product innovation is that frequently the time of development is rather long. New technical and medical knowledge challenge the original invention and thus makes it necessary to adapt the product even before the innovation is marketed (Flessa & Huebner, 2021, 2.1). MedStack allows your organization to stay focused on product and research goals so that you can improve the quality of services and life in healthcare.

Time and Cost Savings

Large-scale IT projects rarely deliver on time, on budget, and on value. On average, large IT projects run 45% over budget, 7% over time, while delivering 54% less value than predicted. Software projects run the highest risk of cost and schedule overruns (Bloch et al., 2012). Often the rush to market means the elimination of scope, corners being cut, misconfigurations, security and compliance violations, and missing or inadequate contingency plans. MedStack eliminates much of this uncertainty and risk so that software projects can focus on what matters: value delivery.

Business Continuity (BC) and Disaster Recovery (DR)

Build with BC and DR to help you remain operational, as a disaster does not wait until it is convenient. MedStack enables you to develop your own Business Continuity and Disaster Recovery Plans with key elements for HIPAA compliance already satisfied. Strengthen yourself against cloud misconfigurations, ransomware, cyberattacks, insider threats, environmental disasters, and more. Test your BC/DR plans early, and test often.

Service Level Agreement (SLA)

Keep your key stakeholders assured and protect their interests with MedStack's SLA. Understand MedStack's responsibilities and obligations, and help set expectations. Our SLA helps to ensure that MedStack is meeting your needs and can help you identify issues early on.

MedStack HIPAA Business Associate Agreement (BAA)

MedStack maintains a BAA with our customers that states that we will protect ePHI in accordance with the requirements set forth by HIPAA. The BAA holds MedStack accountable for violations of HIPAA Security Rules that may occur and outlines the specific duties of the company in safeguarding ePHI.

Third-Party Verified

MedStack undergoes annual audits and works with third-party vendors to maintain our security and compliance posture, including SOC 2 Type 2, Cyber Essentials, Privacy Impact Assessments (PIA), and Threat Risk Assessments (TRA). MedStack's full compliance report package is available to customers to have and share under an equivalent NDA.

ABOUT US

MedStack is a cloud automation technology company built specifically for the needs of the digital health industry. Its standardized platform allows healthcare innovators to deliver ready-to-buy, compliant applications to market and is emerging as the de facto standard for delivering industry requirements for digital health. MedStack has been trusted by hundreds of leading digital health companies around the world and has been accepted in implementation by several notable payers and providers. The company is proudly based in Toronto, Canada.

Authors

Jodie Struthers, Director of Security and Operations
Jodie is the head of MedStack's security and operations team and has been instrumental in building, maintaining, and scaling MedStack's security program into an industry leading example. She is the backbone behind the development of MedStack's secure data systems and the driver of MedStack's robust risk management strategy. Jodie is a seasoned cybersecurity professional with over two decades of experience in technical program management, business strategy development, and security implementation.

Tazeen Naqvi, Privacy and Security Compliance Analyst
Tazeen brings over 6 years of professional compliance management experience to the MedStack team, with prior experience as a consultant and auditor at KPMG. She provides expert compliance and privacy advisory services to all MedStack customers, covering frameworks such as HIPAA, SOC 2, PIPEDA, PHIPA, and GDPR. Tazeen leads MedStack's vendor security questionnaire practice to ensure third-party compliance and runs MedStack's internal compliance program.

REFERENCES

Bloch, M., Blumberg, S., & Laartz, J. (2012, October 1). *Delivering large-scale IT projects on time, on budget, and on value*. McKinsey. Retrieved September 1, 2023, from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

Flessa, S., & Huebner, C. (2021). *Innovations in Health Care-A Conceptual Framework*. International journal of environmental research and public health, 18(19), 10026. https://doi.org/10.3390/ijerph181910026

Marron, J. (2022, July 21). *NIST SP 800-66 Rev. 2 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/66/r2/ipd

National Institute of Standards and Technology. (2022, July 21). *NIST Updates Guidance for Health Care Cybersecurity | NIST*. National Institute of Standards and Technology. Retrieved September 1, 2023, from https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, L., Smith, C., & Steinberg, D. (2008, October). *NIST SP 800-66 Rev. 1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/66/r1/final

U.S. Department of Health and Human Services. (2019, July 22). *Guidance on Risk Analysis*. HHS. Retrieved September 6, 2023, from https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Contact

medstack.co
info@medstack.co
/company/MedStack
@MedStack
877-731-7292

MEDSTACK®