

INTRODUCTION TO HIPAA COMPLIANCE

UNDERSTAND YOUR PATHWAY TO HIPAA COMPLIANCE



securityMETRICS®

ABOUT HIPAA COMPLIANCE

Health Insurance Portability and Accountability Act (HIPAA) compliance includes rules on privacy, security, breach notification, and enforcement with regard to protecting consumer healthcare information. Both Privacy and Security rules require covered entities, business associates, physician/dental practices, pharmacies, and electronic health record (EHR) firms to:

- Implement policies to secure data
- Ensure compliance accountability (Risk Analysis)
- Limit access to Protected Health Information (PHI)
- Conduct workforce training
- Safeguard PHI

Since 1996, HIPAA changed the way organizations create, receive, maintain, and transmit PHI. Efforts to protect United States citizens from data theft, and ensure sensitive healthcare information is only revealed to appropriate parties include the:

- Original HIPAA rule–August 21, 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act–February 18, 2009
- Final omnibus rule – January 25, 2013

These rules provide additional guidance and authority for the Office of Civil Rights (OCR) to enforce HIPAA compliance through audits and financial penalties. The penalties outlined below are per day and per violation. This means that if you have multiple violations you could potentially get fined up to \$50,000 per day for each violation until the violation is resolved. The following chart summarizes compromise and/or noncompliance penalties (Table 1).

VIOLATION CATEGORY	PENALTY	MAXIMUM PER CALENDAR YEAR
(A) Did not know	\$100-\$50,000	\$1,500,000
(B) Reasonable Cause	\$1,000-\$50,000	\$1,500,000
(C) (i) Willful Neglect-Corrected	\$10,000-\$50,000	\$1,500,000
(C) (ii) Willful Neglect-Not Corrected	\$50,000	\$1,500,000

COVERED ENTITIES AND BUSINESS ASSOCIATES

Two groups are required to comply with HIPAA Rules: covered entities and business associates. A covered entity is a health plan, health care clearinghouse or health care provider who electronically transmit any health information. See table below for examples of covered entities.

A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Examples of business associates that typically work with PHI are:

- CPA
- Attorney
- IT providers
- Billing and coding services
- Laboratories
- Claims processing or administration

A HEALTH CARE PROVIDER	A HEALTH PLAN	A HEALTH CARE CLEARINGHOUSE
<p>This includes providers such as:</p> <ul style="list-style-type: none"> • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies <p>...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.</p>	<p>This includes:</p> <ul style="list-style-type: none"> • Health Insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs 	<p>This includes the entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.</p>

HIPAA PRIVACY

The HIPAA Privacy Rule provides federal protections for private protected health information and gives patients an array of rights with respect to that information. The Privacy Rule permits the disclosure of protected health information needed for patient care and other important purposes.

THE HIPAA PRIVACY RULE:

- Spells out administrative responsibilities
- Discusses written agreements between covered entities and business associates
- Discusses the need and implementation for privacy policies and procedures
- Describes employer responsibilities to train workforce members and implement requirements regarding their use and disclosure of PHI

The Privacy Rule applies to all healthcare providers, including those who do not use an EHR, and includes all mediums: electronic, paper, and oral. It gives patients rights to their own protected health information, access to records, and disclosure on how that information is used or shared.



HIPAA SECURITY

The HIPAA Security Rule requires covered entities, business associates, and their subcontractors to implement safeguards to protect electronic protected health information (ePHI) that is created, received, transmitted, or maintained. It specifies a series of administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. Most violations of the HIPAA Security Rule result from businesses not following policies and procedures to safeguard ePHI. The HIPAA Security Rule:

- Establishes a national set of security standards for ePHI
- Protects health information held or transmitted in electronic form
- Requires administrative, physical, and technical safeguards to secure ePHI
- Supports the Privacy Rule requirement to reasonably safeguard PHI in all forms

HIPAA BREACH NOTIFICATION

The Breach Notification Rule requires covered entities, business associates, and their subcontractors to provide notification following a breach of unsecured PHI to affected individuals, the Secretary of Health and Human Services (HHS), and the media (if breach affects more than 500 residents of a State or jurisdiction). The Breach Notification Rule consists of protocols a business must undertake in the event of data compromise. It includes elements such as:

- What constitutes a breach
- Necessary parties to be notified
- Notification timelines
- Notification methods
- Notification content
- Remediation plan

PATHWAY TO HIPAA COMPLIANCE

Most healthcare organizations have been aware of HIPAA Privacy for years and do a pretty good job. The HIPAA Security Rule is often a stumbling block for organizations as it is more technical and really requires a trained security professional. Below are the basic steps on the Pathway to HIPAA Compliance as well as increased data security for both covered entities and business associates.

RISK ANALYSIS

A foundational step in an organization's HIPAA compliance and data security plan is a Risk Analysis. SecurityMetrics HIPAA auditor assists you in identifying all your systems and data flows (i.e. anywhere PHI is created, transmitted, or stored). SecurityMetrics assigns a risk level to each item to create a Risk Analysis Report that gives a snapshot of your organization's risks. This is then used as your Risk Management Plan and is designed to secure your organization as quickly as possible, while at the same time fulfill HIPAA Security Rule compliance requirements. The Risk Analysis is typically conducted onsite at your organization to be as thorough and accurate as possible.

HIPAA GAP ASSESSMENT OF SECURITY, PRIVACY AND BREACH NOTIFICATION

SecurityMetrics HIPAA auditor identifies the gaps between your current compliance level and full HIPAA compliance. You are provided a list of the items identified, prioritized to reduce risk and bring your organization into full HIPAA compliance.

HIPAA COMPLIANCE ASSESSMENT (MOCK OCR AUDIT)

SecurityMetrics HIPAA auditor performs an analysis of your current compliance level. This is a full assessment of the Privacy, Security, and Breach Notification Rules. The auditor discovers your HIPAA compliance status and current compliance gaps. The auditor outlines the steps required to achieve full HIPAA compliance and assists in remediation efforts. The auditor will follow the same protocol an OCR auditor would follow to help prepare you for an OCR audit in the future.

HIPAA CONSULTING

Our HIPAA auditors have the experience and certifications needed to advise on HIPAA and data security related topics. These services can be performed onsite or remotely and assist with your unique circumstances.



PENETRATION TEST

You may have technology in place to prevent data theft, but is it enough to stop criminals? The most accurate way to know is to examine your business environment the same way as hackers, through live testing. SecurityMetrics Penetration Test Analysts manually check your network to find weaknesses that may lead your business to compromise. Leveraging years of experience from onsite assessments, data compromise forensic analysis, and data security consulting, SecurityMetrics Penetration Test Analysts help you achieve security and compliance.

VULNERABILITY SCAN

If left unprotected, thousands of potential entry points on a business network are available for criminals to exploit. As new ways to access these entry points are invented daily, scanning your external business network for vulnerabilities is crucial. SecurityMetrics helps its customers achieve external network security by keeping up with the most current list of vulnerabilities, finely tuning its scan engines to expose weakness, and providing extensive support and remediation assistance.

HIPAA POLICIES AND PROCEDURES

HIPAA policies aren't just paperwork—they are the blueprint to your organization's compliance plan. All employees must be formally trained on HIPAA compliance regularly. SecurityMetrics' policy templates save you time, energy, and money, so you can focus on your organization.

HIPAA TRAINING

Your business is only as secure as its weakest link. SecurityMetrics comprehensive HIPA and Security Awareness trainings help your employees avoid situations that may lead to data breach. These trainings fulfill HIPAA requirements and are easy to use for your employees. Our training console allows you to track employees training status, due dates, and courses completed.

ABOUT SECURITYMETRICS

SecurityMetrics is a global leader in data security and compliance that enables businesses of all sizes to comply with financial, government, and healthcare mandates. Since its founding date, the company has helped over 800,000 organizations protect their network infrastructure and data communications from theft and compromise with exceptional value to customers worldwide. SecurityMetrics HIPAA auditors hold the certification of HealthCare Information Security and Privacy Practitioner. Among other services, SecurityMetrics offers HIPAA assessments, PCI audits, penetration tests, security consulting, data discovery, and forensic analysis.

consulting@securitymetrics.com

801.705.5656

