An Introduction to HIPAA Compliance

securityMETRICS®

Table of Contents

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).

Table 1

Violation Category	Penalty	Total per Calendar Year
(A) Did not know	$100-$50,000	$1.5 Million
(B) Reasonable Cause	$1,000-$50,000	$1.5 Million
(C) (i) Willful Neglect-Corrected	$10,000-$50,000	$1.5 Million
(C) (ii)Willful Neglect-Not Corrected	$50,000	$1.5 Million

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 parities to be notified
- Notification timelines
- Notification methods
- Notification content
- Remediation plan

Additional Rules to HIPAA

HITECH

The HITECH Act increases noncompliance penalties and incentives for covered entities to implement an EHR. It also extends requirements of the HIPAA Security Rule and some aspects of the HIPAA Privacy Rule to business associates. Covered entities are financially penalized or rewarded (EHR Meaningful Use incentive program) for compliance with the HITECH Act.

Final Omnibus Rule

The final omnibus rule, released in January 2013, expands the HIPAA requirements expected of covered entities and business associates and adds subcontractors of business associates that access PHI to the list of organizations that must comply with HIPAA regulations. The rule requires a modification of business associate agreements to include requirements from the final omnibus rule.

The most significant changes to HIPAA from the final omnibus rule affect business associate agreements, business associate subcontractors, fundraising and marketing, hybrid entities, deceased patients records, school immunization records and notices of privacy practices.

Additional HIPAA Compliance Information

HHS Summary of the HIPAA Privacy Rule

HHS Summary of the HIPAA Security Rule

HHS Summary of the HIPAA Breach Notification Rule

HHS Press release of the final omnibus rule

HHS sample business associate agreement provisions

Federal Register of HHS modifications to HIPAA Rules

HHS Summary of the HITECH Act

HHS Wall of Shame (breaches affecting 500 or more individuals)

HIPAA enforcement activities and corrective action plans

SecurityMetrics overview of the HIPAA Security Rule

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 it's founding date, the company has helped over 1 million organizations worldwide protect their network infrastructure and data communications from compromise. Among other services, SecurityMetrics offers HIPAA compliance services, penetration testing, security consulting, payment data discovery, and incident response. Founded in October 2000, SecurityMetrics is a privately held corporation headquartered in Orem, Utah.

If you need assistance with or have further questions about your HIPAA compliance, please email SecurityMetrics at: hipaa@securitymetrics.com.

Stay Current

To stay current on all aspects of business security, subscribe to our YouTube channel, follow us on Twitter, like us on Facebook, and follow us on LinkedIn.

www.youtube.com/securitymetricsinc


www.facebook.com/securitymetrics


www.twitter.com/securitymetrics


www.linkedin.com/company/securitymetrics