Andrew N. Pollak, M.D.
CHAIRMAN

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

Key HITECH Changes to HIPAA

Overview

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded privacy and security regulations established by the Health Information Portability and Accountability Act of 1996 (HIPAA). This included new requirements for breach notification, applicability of HIPAA to business associates (BA), and permitted uses of protected health information (PHI) for marketing and communication purposes, among other things. On January 25, 2013, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published the HIPAA Omnibus Final Rule (Final Rule) requiring compliance by September 23, 2013. The Final Rule strengthens privacy and security protections for PHI that is created, received, maintained or transmitted by a covered entity (CE) or BA.[1]

Timeline

August 21, 1996	• HIPAA passed by Congress
April 14, 2003	• HIPAA Privacy Rule becomes effective
April 21, 2005	• HIPAA Security Rule becomes effective
February 17, 2009	• HITECH signed into law
February 17, 2010	• HITECH enforcement begins to includes financial penalties
January 25, 2013	• HIPAA Omnibus Final Rule published
March 26, 2013	• HIPAA Omnibus Final Rule becomes effective
September 23, 2013	• HIPAA Omnibus Final Rule compliance required

Key Amendments

The Final Rule contains more than 500 pages of rules and provisions. The following list highlights some key modifications made to HIPAA as a result of HITECH. Readers are encouraged to refer to the Final Rule in the Federal Register for a comprehensive overview of the provisions.[2]

Category	Previous HIPAA Standard	Standard as Modified by HITECH
OCR Audits	Audits were not mandatory.	OCR required to conduct periodic compliance audits of CEs and BAs.
CE Definition	CEs include health plans, health care clearinghouses, and health care providers.	Definition expanded to include BAs, such as health information exchanges, regional health information organizations, e-prescribing gateways, subcontractors, and personal health record vendors.
BA Definition	BAs were not subject to the same HIPAA provisions as CEs.	BAs are required to implement administrative, physical, and technical safeguards, and are also subject to civil and criminal penalties for noncompliance.
Use of PHI	Practices could only provide PHI as minimally necessary to accomplish a certain task.	Health care organizations must limit the use, disclosure, or request of PHI, to the extent practicable, specifically to a limited data set or to the minimum necessary. A CE disclosing PHI is required to make the minimum necessary determination.

[1] For more information on the HIPAA Omnibus rule, visit: mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_HIPAA_Omnibus_Rule_Brf_Flyer_20140101.pdf.
[2] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 FR 5566 (January 25, 2013). Available at: www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the.

Category	Previous HIPAA Standard	Standard as Modified by HITECH
	Patient authorization for use of their PHI for marketing purposes was required with three exceptions – CE services, treatment, and case management/alternative treatment.	Patient authorization is required before use or disclosure of their PHI can be made for any marketing purpose.
	Sale of PHI was allowed.	The sale of PHI by CEs and BAs without valid authorization is prohibited with some exceptions – public health activities; research; treatment; services rendered by a BA; or the sale, transfer, merger or consolidation of all or part of a CE.
Disclosure of PHI	CEs were required to account for non-routine disclosures.	CEs must account for all disclosures, including those for treatment, payment, and health care operations. CEs must also account for disclosures made by their BAs or provide individuals with a list of their BAs and their contact information.
		The accounting period for non-routine disclosure of PHI is three years.
		A BA or CE must sign a BA agreement for the release of PHI to an HIE.
Individual Rights	PHI had to be provided to the patient only if it was readily available.	PHI must be provided to a patient (or individuals or entities authorized by the patient) upon request, preferably in electronic format. The fee for providing the PHI cannot exceed the labor cost for providing the PHI.
	CEs were required to account for non-routine disclosures.	Patients may require restrictions on disclosure of their PHI to a health plan where the patient paid out of pocket, in full, for items or services.
	If a patient opts out, CEs had to make a reasonable effort to stop fundraising communications.	If a patient opts out, a CE must stop fundraising communications.
Data Breach Notification	CEs and BAs had no direct obligation for notification if there was a data breach.	Upon discovery of a suspected breach, CEs must notify HHS; prominent media outlets (if more than 500 patients are affected); and patients (within 60 days). There are limited exceptions for unintentional access by employees and inadvertent disclosures within an office.[3]
		Consumer notification of data breaches involving "unsecured" PHI or information not secured through the use of technology or methodology specified in guidance by HHS is required.
		Vendors of PHI and their service providers are also subject to security breach notification requirements.
Data Breach Enforcement	Investigation of a data breach was collaborative between OCR and a CE.	Collaborative investigation involving OCR and a CE expanded to include individual employed at the CE and their BA(s).
		An OCR investigation is required to determine willful neglect.[4]
Data Breach Penalties	Penalties ranged from a minimum of $100 to a maximum of $25,000.	Fines for data breach are $100 to $50,000 per violation (or record), with yearly maximum of $25,000 to $1.5 million.
		OCR must investigate any complaint related to a violation that may have resulted from willful neglect. If a violation is determined, OCR must assess civil monetary penalties. Violations can also carry criminal charges.
		Corrective action can be required in lieu of a penalty if the CE or BA is unaware that a violation occurred.
Patient Education	No patient education requirements.	Established educational initiative to provide education on health information privacy. A privacy advisor is designated in each of the 10 HHS regional offices.[5]
Electronic Media Definition	Limited to storage media, such as tape or disk.	Expanded to include Internet and VoIP technology.

[3] More information on data breach notification and relevant exceptions can be found at: www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[4] The conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[5] More information about HHS regional offices is available at: www.hhs.gov/about/agencies/regional-offices/index.html.