Chapter 7: Breach Notification, HIPAA Enforcement, and Other Laws and Requirements

Covered Entities (CEs) and Business Associates (BAs) that fail to comply with Health Insurance Portability and Accountability Act (HIPAA) Rules can receive civil and criminal penalties.

Civil Penalties

The Office for Civil Rights (OCR) is able to impose civil penalties for organizations that fail to comply with the HIPAA Rules. The potential civil penalties are substantial. Your good faith effort to be in compliance with the HIPAA Rules is essential.

State attorneys general also may bring civil actions and obtain damages on behalf of state residents for violations of the HIPAA Rules. [1] Learn more about OCR's HIPAA enforcement; [2] HIPAA Privacy, Security, and Breach Notification Audit Program;[3] and HIPAA Enforcement Rule.[4]

Criminal Penalties

The U.S. Department of Justice investigates and prosecutes criminal violations of HIPAA. Under HIPAA, the Justice Department can impose criminal penalties for:

- Knowing misuse of unique health identifiers.[5]
- Knowing and unpermitted acquisition or disclosure of Protected Health Information (PHI).[6]

Oversight

OCR, within the U.S. Department of Health and Human Services (HHS), administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules. OCR conducts complaint investigations, compliance reviews, and audits. OCR may impose penalties for failure to comply with the HIPAA Rules.

The Centers for Medicare and Medicaid Services (CMS) within HHS oversees the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs.

The Office of the National Coordinator for Health Information Technology (ONC) provides support for the adoption and promotion of health information technology (health IT) and Health Information Exchanges (HIEs) to improve health care in the United States.

The Breach Notification Rule: What to Do If You Have a Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of unsecured PHI is presumed to be a

[1] This authority was granted to state attorneys general in the Health Information Technology for Economic and Clinical Health (HITECH) Act.
[2] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
[3] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html
[5] HIPAA regulations specify the appropriate use of identifiers.
[6] The HIPAA Privacy Rule establishes what is an impermissible obtainment or disclosure of PHI.

breach unless the CE or BA demonstrates (based on a risk assessment) that there is a low probability that the PHI has been compromised.[7] When a breach of unsecured PHI occurs, the Rules require your practice to notify affected individuals, the Secretary of HHS, and, in some cases, the media.[8]

The Breach Notification Rule requires HIPAA CEs to notify individuals and the Secretary of HHS of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI. In particular, health care providers must promptly notify the Secretary of HHS if there is any breach of unsecured PHI that affects 500 or more individuals, and they must notify the media if the breach affects more than 500 residents of a state or jurisdiction. If a breach affects fewer than 500 individuals, the CE must notify the Secretary and affected individuals. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- Significant breaches are investigated by OCR, and penalties may be imposed for failure to comply with the HIPAA Rules. Breaches that affect 500 or more patients are publicly reported on the OCR website.[9]
- Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to Personal Health Record (PHR) developers and their third-party service providers.

If you can demonstrate through a risk assessment that there is a low probability that the use or disclosure compromised unsecured PHI, then breach notification is not necessary. (Please note that this breach-related risk assessment is different from the periodic security risk analysis required by the Security Rule).

And, if you encrypt your data in accordance with the OCR guidance regarding rendering data unusable, unreadable, or indecipherable, you may avoid reporting what would otherwise have been a reportable breach. Remember, encryption depends on the encryption key being kept highly confidential, so do not store it with the data or in a location that would compromise it.[10]

Table 1 compares secured and unsecured PHI.

Table 1: Comparison of Secured and Unsecured PHI

Secured PHI	Unsecured PHI
An unauthorized person cannot use, read, or decipher any PHI that he/she obtains because your practice: • Encrypts the information; or • Clears, purges, or destroys media (e.g., data storage devices, film, laptops) that stored or recorded PHI; • Shreds or otherwise destroys paper PHI. (These operations must meet applicable federal standards.[11])	An unauthorized person may use, read, and decipher PHI that he/she obtains because your practice: • Does not encrypt or destroy the PHI; or • Encrypts PHI, but the decryption key has also been breached.

[7] http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
[8] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[9] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[10] Federal Register (FR). (24 August, 2009). Rules and Regulations. II.A. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (Vol. 74, No. 162). Paragraph 3, pp. 42741-42.
[11] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

Risk Assessment Process for Breaches

When you suspect a breach of unsecured PHI has occurred, first conduct a risk assessment[12] in order to examine the likelihood that the PHI has been compromised. For you to demonstrate that a breach has not compromised PHI, your practice must conduct the risk assessment in good faith and by thoroughly assessing at least the four required elements[13] listed below.

- The nature and extent of the PHI involved in the use or disclosure, including the types of identifiers and the likelihood that PHI could be re-identified
- As noted above, if your practice has a breach of encrypted data — and if you had followed standard encryption specifications — it would not be considered a breach of unsecured data, and you would not have to report it.
- The unauthorized person who used the PHI or to whom the disclosure was made (e.g., a sibling or a journalist)
- The likelihood that any PHI was actually acquired or viewed (e.g., an audit trail would provide insights)
- The extent to which the risk to the PHI has been mitigated (e.g., promptly changed encryption key)

When performing this assessment, you should address each element separately and then analyze the combined four elements to determine the overall probability that PHI has been compromised.

The conclusions from your assessment must be reasonable. You have the burden of demonstrating that a use or disclosure of unsecured PHI did not constitute a breach. If this assessment indicates that there is:

- Low probability of compromised PHI, then the use or disclosure is not considered to be a breach and no notification is necessary.
- Probability of compromised PHI, breach notification is required.

[12] 45 Code of Federal Regulations (CFR) 164.402(2); http://www.ecfr.gov/cgi-bin/text-idx?SID=938e08839465e82e2c30c3bd4a359ce2&node=pt45.1.164&rgn=div5#se45.1.164_1402

[13] The four elements are taken from the "Definition of Breach" section at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/.

Reporting Breaches

If you choose not to conduct the risk assessment, or if, after performing the risk assessment outlined above, you determine that breach notification is required, there are three types of notification to be made to individuals, to the Secretary of HHS, and, in some cases, to the media. The number of individuals that are affected by the breach of unsecured PHI determines your notification requirements. Visit the OCR Breach Notification Rule web page[14] for more information on notifying individuals, the Secretary, and the media.

If you determine that breach notification is required, you should also visit the OCR website for instructions[15] on how to submit the breach notification form[16] to the Secretary of HHS. Once notified, HHS publicly reports, on the OCR website,[17] breaches that affect 500 or more individuals. OCR opens a compliance review of all reported breaches that affect 500 or more individuals and many breaches affecting fewer than 500. (Note that similar breach notification provisions, which are implemented and enforced by the Federal Trade Commission,[18] apply to developers of PHRs that are *not* providing this service for a CE.)

Investigation and Enforcement of Potential HIPAA Rules Violations

OCR initiates investigations upon receipt of complaints,[19] breach reports, information provided by other agencies, and the media. The HIPAA Enforcement Rule provides different penalties for each of four levels of culpability:

- Violations that the entity did not know about and would not have known about by exercising reasonable diligence
- Violations due to "reasonable cause"
- Violations due to "willful neglect" that are corrected within 30 days
- Violations due to "willful neglect" that are not corrected within 30 days[20]

Penalties for Violations

Table 2 provides an overview of the penalty amounts for HIPAA violations. Contact your legal counsel for specific guidance.

[14] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
[15] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[16] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
[17] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
[18] http://www.consumer.ftc.gov/
[19] http://www.hhs.gov/ocr/privacy/hipaa/complaints/
[20] 45 CFR 160.404.

Table 2: Overview of Penalties

Intent	Minimum Per Incident	Annual Cap for All Violations
Did Not Know or Could Not Have Known	$100 – $50,000	$1.5 million
Reasonable Cause and Not Willful Neglect	$1,000 – $50,000	$1.5 million
Willful Neglect, but Corrected Within 30 Days	$10,000 – $50,000	$1.5 million
Willful Neglect and Not Corrected Within 30 Days	$50,000	$1.5 million

In addition to investigations that OCR conducts for potential violations of the HIPAA Rules, the HITECH Act authorizes and requires HHS to conduct periodic audits to ensure that CEs and BAs comply with the HIPAA Rules.[21] Audits are not initiated because of any particular event or incident, but rather due to application of a set of objective criteria. HHS uses these audits as a way to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews.

Other Laws and Requirements

Besides HIPAA Rules, HITECH, and Meaningful Use privacy- and security-related requirements, your medical practice may also need to comply with additional privacy and security laws and requirements. Table 3 provides a snapshot of these domains. Your state, state board of medicine, state associations, Regional Extension Center (REC), and HIE initiatives also may have guidance.

Table 3: Overview of Other Laws and Requirements

Laws/Requirements	Key Points

Sensitive Health Information	• Some laws and frameworks recognize that particular health conditions may put individuals at a higher risk for discrimination or harm based on that condition. Federal and some state laws require special treatment and handling of information relating to alcohol and drug abuse, genetics, domestic violence, mental health, and Human Immunodeficiency Virus (HIV)/Acquired Immune Deficiency Syndrome (AIDS).
	• Applicable federal laws:
	  ○ 42 CFR Part 2: Confidentiality of Alcohol and Drug Abuse
	  ○ Family Educational Rights and Privacy Act (FERPA)
	  ○ Title X of Public Health Service Act — Confidentiality

Adolescent/ Minors' Health Information	• State and federal laws generally authorize parent or guardian access.
	• Depending on age and health condition (e.g., reproductive health, child abuse, mental health) and applicable state law, minors also have privacy protections related to their ability to consent for certain services under federal or state law.
	• Applicable federal laws:
	  ○ FERPA
	  ○ Genetic Information Nondiscrimination Act (GINA)
	  ○ Title X of Public Health Service Act
	Note: The HIPAA Omnibus Rule clarified that CEs may release student immunization records to schools without authorization if state law requires schools to have immunization records and written or oral agreements (must be documented).

Private Sector	A contracting health plan or payer may require additional confidentiality or safeguards.

[21] HITECH Act, Section 13411.

A good place to start privacy- and security-related compliance implementation within your practice is to:

- Stay abreast of privacy and security updates. Sign up for OCR's privacy and security listservs[22] to receive updates, and contact your local association to learn about available assistance sources.
- Integrate privacy and security updates into your policies and procedures.
- Identify and monitor violations and demonstrate good faith efforts to promptly cure any violation that may occur.

[22] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html