MYTH: HIPAA is not actively enforced.

FACT: The HHS Office for Civil Rights enforces the HIPAA Privacy and Security Rules by investigating complaints filed by patients, conducting audits, and allowing state attorneys general to bring a civil action on behalf of state residents for alleged HIPAA violations.

Patients who believe that their health information privacy rights under the HIPAA Privacy, Security or Breach Notification Rules have been violated by a covered entity or business associate, may file a complaint with the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR).[1]

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[2] made several modifications to the enforcement process under HIPAA. These changes were codified in the Omnibus Final Rule published by HHS on January 17, 2013.[3]

Importantly, the HIPAA Omnibus Rule replaces the "harm" standard with a new standard called "LoProCo (Low Probability of Compromise)" to determine whether there has been a breach. The new standard states that the impermissible use or disclosure of PHI is presumed to have occurred triggering notification requirements, unless the covered entity or business associate can demonstrate low probability that PHI has been compromised by a risk assessment of:

- The nature and extent of PHI involved;
- Who received or accessed the information;
- The potential that the PHI was actually acquired or viewed;
- Extent to which risk to the data has been mitigated.

The HITECH Act also authorizes state attorneys general to bring civil actions on behalf of state residents who have been adversely affected by alleged violations of the HIPAA Privacy and Security Rules. State attorneys general may either collect damages on behalf of state residents or may protect residents against further violations of the Privacy and Security Rules.[4]

In addition to their enforcement duties, the HITECH Act also authorizes OCR to conduct periodic audits to ensure compliance with HIPAA. Audits allow OCR to ensure mechanisms for compliance, identify best practices, and discover additional risks and vulnerabilities not seen in compliance reviews or investigations. To date, OCR has conducted audits of 115 entities.[5]

OCR has been very active investigating and penalizing violations of the HIPAA Rules. Since 2003, 85,239 complaints have been filed, 30,886 complaints have been investigated, and since 2008, $17.6 million in civil money penalties and resolution agreements have been collected.

For More Information:

- Learn about state and federal laws related to privacy.
- Read our overview of HIPAA and related resources.

Follow us on Twitter at @HealthInfoLaw

---

[1] More information on the complaint process can be found here: Myth Buster on HIPAA Private Right of Action.

[2] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), Division A, Title XIII and Division B, Title IV, Health Information Technology for Economic and Clinical Health Act (HITECH Act) (codified at 42 U.S.C. § 17930, et seq).

[3] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the

HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) (to be codified at 45 CFR pts 160 and 164).

[4] 42 U.S.C. § 17939.

[5] HIPAA Privacy, Security and Breach Notification Audit Program, Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.