How is HIPAA Enforced?

The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services is responsible for enforcing the Health Insurance Portability and Accountability Act's (HIPAA) Privacy and Security Rules. OCR's enforcement process includes:

- Investigation of complaints filed by an individual;
- Compliance reviews of entities who must comply with HIPAA Rules; and
- Education and outreach to foster compliance with the Privacy and Security Rules.

Under the Health Information Technology for Economic and Clinical Health (HITECH) Act state attorneys general also have the authority 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 collect damages on behalf of state residents, and are authorized to bring civil actions against HIPAA violators if the violation threatens or adversely affects a state resident.[1]

Once a complaint is filed with OCR, an investigation takes place to determine whether a violation of the Privacy or Security Rules has occurred. OCR will either find that no violation has occurred, obtain voluntary compliance, corrective action or other arrangement, or issue a formal finding of a violation. OCR also may require the offending entity to pay a civil money penalty (CMP). The HITECH Act strengthened HIPAA enforcement by establishing four categories of violations with increasing levels of culpability, four tiers of increasing penalty amounts, and a maximum penalty of $1.5 million for all violations of an identical provision.[2] Alternatively, if OCR finds evidence of a possible criminal violation during the intake process, it will refer the case to the U.S. Department of Justice, which may impose criminal penalties on a covered entity or business associate subject to the HIPAA Rules.

As of November, 2013, OCR has investigated 21,763 cases, and required changes in privacy practices or other corrective actions. The most common compliance issues that OCR investigates are:

1. Impermissible use and disclosure of protected health information;
2. Lack of adequate safeguards of protected health information;
3. Lack of patient access to their own protected health information;
4. The use and disclosure of protected health information that is more than minimally necessary; and
5. Lack of administrative safeguards of electronic health information.

Noteworthy HIPAA Enforcement Actions:

- $4.3 million CMP against Cignet Health for Privacy Rule violations (February 2011)
- $1.5 million settlement with Blue Cross Blue Shield of Tennessee for potential Privacy and Security Rule violations (March 2012)
- $1.7 million settlement with Alaska Department of Health and Human Services for potential Security Rule violations (June 2012)
- $1.7 million settlement with Wellpoint for potential Privacy and Security Rule violations (July 2013)

For more information on state and federal laws related to privacy, see www.healthinfolaw.org/topics/63.
For more information about HIPAA, see www.healthinfolaw.org/federal-law/HIPAA.
Follow us on Twitter at **@HealthInfoLaw**

[1] 42 U.S.C. § 17939.
[2] HITECH Act § 13410(d), amending 42 U.S.C. § 1320d-5.