

HIPAA Breach Notification: Recent Enforcement Actions

Three years have passed since the Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted, adding HIPAA Breach Notification requirements to a long list of privacy-related obligations imposed on health care entities. To date, nine separate entities have incurred more than \$12 Million in fines and penalties from breaches and other HIPAA violations.

Many of these fines could have been avoided if the company (or “entity”) had established policies and procedures to ensure it met all regulatory requirements, or if the company’s workforce had followed such policies. Where computer theft or loss was involved, costly notifications and fines related to a breach could have been avoided if proper encryption had occurred.

Here is a summary of federal enforcement actions occurring since HITECH became law:

Breach Incident/violation	Fine/Penalties	Entity Name	Entity Description
Improper disposal of PHI	\$1 Million	Rite Aid Pharmacy	Large pharmacy retail chain
Use of PHI for marketing purposes without an authorization	\$35,000	Management Services Organization Washington, Inc.	Healthcare management company
Denied patients access to their medical records	\$4.3 Million	Cignet Health, Inc.	Multi-site healthcare facility
Lost fee tickets/billing forms on subway train	\$1 Million	Massachusetts General Physicians Organization	Hospital and physician organization
Impermissible access to patient records	\$865,500	University of California Los Angeles Health System	Academic medical center
Stolen hard drives	\$1.5 Million	Blue Cross Blue Shield of Tennessee	Large health insurance carrier
Posted surgery appointments on publicly-available Internet-based calendars	\$100,000	Phoenix Cardiac Surgery, P.C.	Cardiac surgery practice group
Stolen flash drive	\$1.7 Million	Alaska Dept of Health and Social Services	State health agency
Stolen lap top computer	\$1.5 Million	Massachusetts Eye and Ear Associates, Inc.	Ophthalmology practice group

The Office of Civil Rights (OCR), under the Department of Health and Human Services, is charged with enforcing all HIPAA regulations, including the recent HITECH Act. There are several reasons to believe that enforcement of HITECH is not going away any time soon:

1. With each passing year, the number of facilities receiving enforcement actions has increased, due to a HITECH provision that allows fines and penalties received under HITECH to be used by OCR to expand its enforcement efforts. Thus, with each fine levied there is the opportunity for OCR to hire more staff and/or expand its scope of investigations and audits.
2. OCR has awarded a \$9 Million contract to KPMG, to help audit HIPAA Privacy and Security compliance by covered entities and their business associates. Those audits are on-going and early results indicate this model to be an effective means for OCR to monitor privacy compliance across a wide range of entities.
3. Under HITECH, States Attorneys General are given specific authority to bring civil actions for HIPAA violations and to obtain damages on behalf of state residents when violations have occurred. OCR has already introduced a HIPAA enforcement training program specifically for States Attorneys General.

Nonetheless, there is much that you can do to help avoid similar enforcement actions:

1. Learn and follow the HIPAA policies and procedures specific to your organization.
2. Know and respect the privacy rights of patients served by your organization.
3. Protect the privacy and security of all patient information entrusted to you. Take special care to encrypt all portable electronic devices that might contain sensitive or protected health information.
4. Report suspected violations or breaches immediately by calling your privacy official.

To learn more about HIPAA enforcement process or what you can do to avoid HIPAA breaches, contact the University of Louisville [Privacy Office](#) at (502) 852-3803 or privacy@louisville.edu.