THE OFFICIAL NEWSMAGAZINE OF THE AMERICAN ACADEMY OF PEDIATRICS
AAP News

News Articles, Health IT Trends

Physician offices hit with penalties for HIPAA violations

by from the AAP Division of Health Care Finance

Pediatricians in office practices who believe they don't need to worry about privacy and security investigations related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) had better think again.

HIPAA enforcement has begun exposing all covered entities (e.g., physician offices, clinics, hospitals, etc.) to civil and criminal penalties if proper administrative, technological and physical controls to protect privacy and security are not followed.

Private practices are the most common type of covered entities that have been required to take corrective action to achieve voluntary HIPAA compliance. Other covered entities in order of frequency are general hospitals, outpatient facilities, pharmacies and health plans (group health plans and health insurance issuers).

While the U.S. Department of Health and Human Services set the HIPAA regulations, the Office of Civil Rights (OCR) enforces them by investigating complaints and determining whether the covered entity is in compliance. If the OCR determines that no violation exists, the findings are documented and the case is closed. However, if violations are identified, the covered entity may be required to take one or more of the following actions: implement voluntary compliance (i.e., develop, implement and use internal controls to monitor HIPAA adherence) or enter into a resolution agreement (a contract signed by the covered entity and OCR, obligating the entity to perform various compliance-related tasks and submit to monitoring for up to three years). Corrective action plans specifying how the compliance plan will be implemented often accompany the resolution agreement.

Fines are imposed in some cases, and criminal penalties occur in extreme situations (see table).

Following are examples of recent HIPAA enforcement actions:

THE OFFICIAL NEWSMAGAZINE OF THE AMERICAN ACADEMY OF PEDIATRICS
AAP News

News Articles, Health IT Trends

- A 12-physician pediatric and adult dermatology practice group paid $150,000 for alleged HIPAA violations arising out of a lost, unencrypted flash drive containing protected health information (PHI). The group also was required to implement a corrective action plan.
- A five-physician cardiology group reached a $100,000 settlement as a result of a multiyear, ongoing failure to comply with the HIPAA privacy and security requirements by posting clinical and surgical appointments for patients on a publicly accessible internet-based calendar. The practice had failed to implement even the most basic HIPAA requirements, such as adopting policies and procedures to safeguard patient information appropriately.
- An orthopedic clinic failed to execute a business associate agreement prior to turning over 17,300 patients' PHI to a potential business partner. The settlement included a monetary payment of $750,000 and a comprehensive corrective action plan.

When determining penalties, the OCR takes into account the length of time a violation persisted, the number of people affected, the nature of the PHI exposed and the organization´s willingness to assist with the investigation.

Pediatric practices must have HIPAA privacy and security compliance programs (see resource). They also must conduct periodic internal risk assessments to reveal gaps and address them.

Many practices are purchasing cyber liability insurance, a relatively new type of insurance policy that protects against data breaches by covering the costs of:

- contacting customers after a breach of private information;
- hiring information technology forensic specialists to investigate a breach and figure out where the leak occurred;
- deploying public relations/marketing professionals to handle the community messaging required by certain breaches;
- providing credit monitoring for patients whose records were exposed; and
- HIPAA fines.

Not all cyber liability policies cover HIPAA fines, and some may limit coverage based on the nature of the HIPAA violation. For instance, a $1 million policy may allow $200,000 to be spent on HIPAA fines.

HIPAA violations and penalties

Civil

Violation	Penalty
The covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation*
The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation*

THE OFFICIAL NEWSMAGAZINE OF THE AMERICAN ACADEMY OF PEDIATRICS
AAP News

News Articles, Health IT Trends

The HIPAA violation was due to willful neglect, but the violation was corrected within the required time period.	$10,000-$50,000 for each violation*
The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation*

* Up to a maximum of $1.5 million for identical provisions during a calendar year

Criminal

Violation	Penalty
Unknowingly or with reasonable cause	Up to one year in prison
Under false pretenses	Up to five years in prison
For personal gain or malicious reasons	Up to 10 years in prison

Source: Health Information Technology for Economic and Clinical Health Regulations - Section 13410(d)

Resource

- AAP members can download free pediatric-specific privacy and security compliance manual templates. Each practice must tailor the manuals to its specific operations.