Are Your Clients HIPAA COMPLIANT?

The Department of Health and Human Services is tasked with ensuring health care organizations are compliant with HIPAA regulations regarding patient data, and it has stepped up its efforts to oversee compliance in 2016 and 2017.

HIPAA, or the Health Insurance Portability and Accountability Act, was enacted in 1996 to protect the privacy and security of patient health data. The Department of Health and Human Services' Office of Civil Rights (OCR) is currently working to ensure that health care providers, insurance companies and other covered entities, as well as their business associates (including lawyers, consultants and cloud storage providers) are carefully following HIPAA standards. Attorneys need to ensure that their clients are aware of this renewed focus and are taking the steps necessary to keep themselves fully compliant.

Statistics on HIPAA Violations

A HIPAA audit that unearths noncompliance can mean:

- Steep fines
- Negative impacts on business revenue
- Damaged reputation

Examples of recent substantial settlements

within the health care industry following HIPAA citations of noncompliance:

Triple-S Management Corporation

(insurance holding company based in Puerto Rico)

Paid $3.5 million for several HIPAA violations, including:

- Allowing record access to an ex-employee
- Employee-to-employee transfer of patient health information via computer
- Mailing insurance ID cards to incorrect patients and including important numbers on mailings

Lahey Hospital and Medical Center

(Burlington, Massachusetts)

Paid $850,000 for violations, including:

- A data breach resulting from the disappearance of an unencrypted laptop from an unlocked room inside the hospital's radiology department
- An OCR investigation prompted by the data breach revealed the lack of a process within the facility surrounding the deep risk analysis of its online patient health information

University of Washington Medicine

Paid $750,000 for violations, including:

- Compromising the health information of up to 90,000 patients when an employee inadvertently downloaded malware from an email attachment
- Failure to ensure that all affiliated partners were overseeing risk assessments of their own systems

What a HIPAA Phase 2 Audit Covers

OCR announced in July 2016 that **167 health care organizations would be investigated** for Phase 2 of its audit program

OCR will be auditing both **health care organizations** and their "**business associates**," (i.e., attorneys, consultants, cloud storage companies and anyone else who manages online patient health care data on behalf of the main covered health care entities)

OCR has announced that the Phase 2 audits will attempt to collect **best practices** as well as uncover **new security vulnerabilities**

Approximately **180 different criteria** may be addressed in an audit. Broadly speaking, they cover:

Physical safeguards, such as:

- Making sure doors are locked
- The use of access badges
- Installing surveillance cameras

Technical safeguards, such as:

- Password protection for each user
- Comprehensive encryption
- Regular backups
- Disaster recovery plan

Administrative safeguards, such as:

- Ensuring business associates and contractors are HIPAA compliant
- Creating a process for auditing data

A few of the most common HIPAA violations include:

- Failing to send records to patients in a timely manner when requested
- Failing to shred physical records or electronically wipe them when they need to be disposed of
- Failing to secure patient signatures on records
- Releasing records to unauthorized viewers
- Sending the incorrect patient's information

How Attorneys Can Help Ensure HIPAA Compliance

Attorneys can help ensure their health care organization clients are fully prepared for an audit by suggesting a few key measures:

- Take the HIPAA compliance self-assessment provided by the Department of Health and Human Services
- Make certain all patient health information is securely encrypted
- Organize comprehensive employee training sessions to ensure employees are HIPAA compliant

Clyde Bennett, the chief health care technology strategist for Aldridge Health, recommends that any organization covered by HIPAA ask itself the following key questions:

- "Does my business have written policies and protocols in place to address HIPAA standards?"
- "Is my business performing and documenting regular risk assessments?"
- "Does my business have an established data security policy?"
- "Are the business associates affiliated with my organization HIPAA compliant?"
- "Does my business have an effective incident response plan to handle a breach if it occurs?"
- "Are my employees required to complete regular HIPAA training programs?"

MAURICE A. DEANE SCHOOL OF LAW
HOFSTRA LAW

SOURCES:

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/
http://www.americanbar.org/publications/aba_health_esource/2016-2017/september2016/phase2audit.html
http://healthitsecurity.com/news/ensuring-hipaa-compliance-before-a-potential-hipaa-audit

HEALTHLAW.HOFSTRA.EDU