Common HIPAA violations physicians should guard against

MAR 3, 2021

Andis Robeznieks
Senior News Writer

From the Hippocratic Oath of ancient Greece to modern Washington's Health Insurance Portability and Accountability Act (HIPAA), patient privacy has been a foundation of medicine and is etched into the AMA *Code of Medical Ethics*.

"Protecting information gathered in association with the care of the patient is a core value in health care," states opinion 3.1.1 of the *Code*. "However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust."

The AMA describes HIPAA as establishing "guardrails for the sharing and use of patient health information" between health care providers. The AMA notes that HIPAA regulations are mainly "permissive" in that they allow, but don't *require,* the sharing of health information. And, generally, physicians and hospitals may share patient information without explicit patient consent for treatment, payment, and business operations reasons.

Crossing the lines established by HIPAA can result in civil penalties ranging from $100 for an "unknowing" violation to $1.5 million for "willful neglect." The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) is responsible for enforcing compliance with HIPAA privacy rules.

For more than 15 years, the OCR has tracked the most-often alleged compliance issues included in HIPAA complaints.

According to the OCR, they are:

- Impermissible uses and disclosures of protected health information.
- Lack of safeguards of protected health information.
- Lack of patient access to their protected health information.
- Lack of administrative safeguards of electronic protected health information.
- Use or disclosure of more than the minimum necessary protected health information.

Physicians and private practices are alleged to be the second-most common violator of HIPAA privacy regulations, coming in behind hospitals and ahead of outpatient facilities, pharmacies and health plans, the OCR says.

Last year, the OCR launched its HIPAA Right of Access Initiative promising to “vigorously enforce the rights of patients to get access to their medical records promptly without being overcharged, and in the readily producible format of their choice.”

So far, the initiative has settled 15 investigations.

The AMA has released a patient access playbook to help physicians better understand their obligations under HIPAA to provide patients with access to their information.

Feds seek voluntary compliance

The OCR typically tries to resolve cases by obtaining voluntary compliance, through a corrective action, or with a resolution agreement.

The HHS website describes a case in which a patient's HIV status was disclosed after an employee at a doctor's office mistakenly faxed medical records to the patient's workplace instead of to the patient's new health care provider.

“The employee responsible for the disclosure received a written disciplinary warning, and both the employee and the physician apologized to the patient,” the website states. “To resolve this matter, OCR also required the practice to revise the office's fax cover page to underscore a confidential communication for the intended recipient.”

No fine is mentioned in that case. Civil penalties for violations have totaled almost $112 million since 2003. The OCR has referred 824 criminal violations to the Department of Justice to investigate.

Entities that knowingly obtain or disclose individually identifiable health information in ways not permitted by HIPAA may face a fine of up to $50,000, as well as imprisonment up to one year, according to AMA HIPAA resources.

Offenses committed under false pretenses allow penalties to be raised to a $100,000 fine, with up to five years in prison. Intending to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm can result in fines of $250,000 and imprisonment up to 10 years.

Cyber thieves see data as commodity

Patients' digital medical records are 50 times more valuable than financial information, according to cybersecurity experts. And the AMA believes that keeping the patient at the center of care requires steadfast adherence to their rights to privacy.

"Without appropriate safeguards, patients' data could become a commodity, the AMA health data privacy framework states. "Health data can provide a wealth of information for marketers or be sold and exchanged by data brokers—impacting insurance coverage, access to care, or resulting in employment discrimination."