HIPAA' s Criminal Charges Pack a Heavy Punch

Insights
2.02.15

Almost all healthcare providers and health plan administrators are familiar with the detailed requirements of the privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA). Violations can result in significant monetary penalties. But HIPAA violations can also result in criminal charges. And the frequency of alleged criminal violations appears to be increasing.

In August 2014, Joshua Hippler, a former hospital employee in East Texas, pled guilty to criminal HIPAA violations after he was indicted on charges of wrongful disclosure of individually identifiable health information. Hippler faces up to 10 years in federal prison.

In the ever-expanding digital world, more and more healthcare providers have moved away from paper records in favor of electronic medical records. Many in the healthcare industry predict that this shift will propel more criminal prosecutions as the digital age makes accessing patient information as easy as the click of a button.

HIPAA Penalties
HIPAA provides for both civil penalties and criminal penalties for violating the Act. The Department of Health and Human Services (HHS) is charged with enforcing civil penalties of HIPAA violations, while the U.S. Justice Department (DOJ) is charged with criminal prosecution of HIPAA violations.

The HIPAA criminal statute provides that:

A person who knowingly and in violation of this part –

1. uses or causes to be used a unique health identifier;
2. obtains individually identifiable health information relating to an individual; or
3. discloses individual identifiable health information to another person, shall be punished as provided in subsection (b) of this section.

In *U.S. v. Zhou*, the U.S. Court of Appeals for the 9th Circuit clarified that the "knowingly" element in the HIPAA statute only requires knowledge of the action that constitutes the offense (*i.e.*, accessing a patient's protected health information), not knowledge that the conduct is a violation of HIPAA. Huping Zhou, a former research assistant at the University of California at Los Angeles Health

System, accessed patient records without authorization after he was terminated. Zhou also accessed confidential health records of his supervisor, coworkers, and even several celebrities during the weeks following his termination. Zhou's defense was premised on the argument that he did not know it was illegal to obtain private health information and therefore could not "knowingly" violate the statute.

The court did not agree with Zhou's interpretation of the statute. The three-judge panel ultimately concluded that the law's protection is not limited to defendants who knew that their actions were illegal. Rather, the defendant need only know that he obtained individually identifiable health information relating to an individual. In other words, knowingly obtaining or disclosing private health information is enough to violate HIPAA and face criminal liability.

Are Healthcare Providers Subject to Criminal Penalties?

While the majority of HIPAA criminal charges to date have been lodged against individual employees, covered entities (*i.e.,* health plans, healthcare providers that submit electronic claims, healthcare data clearinghouses) can also be criminally prosecuted under HIPAA.

It's even conceivable that a corporate entity could face criminal charges for having inadequate policies and procedures in place to prevent unauthorized access of a patient's individually identifiable health information. A covered entity's knowledge of an employee's unauthorized access or disclosure of a patient's protected health information may also trigger criminal liability. Such lapses would certainly expose the covered entity to various civil penalties.

Covered entities and individuals who "knowingly" obtain or disclose individually identifiable health information face a fine of up to $50,000 and imprisonment for up to one year. The penalties may be increased to a fine of $100,000 with up to five years in prison for offenses committed under false pretenses. Finally, if a covered entity or individual "knowingly" obtains or discloses individually identifiable health information with the intent to sell, transfer or use the protected data for commercial advantage, personal gain or malicious harm, they could face up to ten years in prison and a fine of $250,000.

How to Ensure Patients' Privacy (And Avoid Liability under HIPAA)

Employers in the healthcare field can reduce their liability by implementing safeguards such as auditing employees' access to patient records and creating an internal log which forces employees to "state the reason" for accessing a patient's record.

With social media permeating our personal, and oftentimes, professional spheres of life, it is important to remember that some employees may have a narrower view of what type of information is private. You can combat this by training employees on patient privacy and reinforcing HIPAA' s requirements. It would also be wise to distribute material which explains the criminal penalties that employees face for HIPAA violations.

Now more than ever, it's paramount for covered healthcare entities to develop health information security compliance programs which convey a zero-tolerance policy for security violations. You

security compliance programs which convey a zero-tolerance policy for security violations. You should also document employees' understanding and acknowledgment of the confidentiality policies maintained by your facility.

And, of course, act immediately upon any information or indication that an employee is accessing or using protected health information in violation of HIPAA.

For more information, contact the author at AMiller@fisherphillips.com or (908) 516-1050.

Service Focus

Privacy and Cyber

Industry Focus

Healthcare