HIPAA Enforcement On The Rise

Insights
8.03.15

The number of claims filed under the Health Insurance Portability and Accountability Act (HIPAA) have skyrocketed in recent years. The latest figures from the U.S. Department of Health and Human Services (DHS) highlight a dramatically increased enforcement effort by the government in administering the federal privacy law.

According to the U.S. Office of Civil Rights (OCR), it has received over 115,929 HIPAA complaints and initiated over 1,216 compliance reviews since the promulgation of the final HIPAA Privacy Rule in 2013. Of those, 23,580 have required businesses to make changes to their privacy practices or otherwise face corrective actions.

Colorado Pharmacy Learns The Hard Way
One such recent settlement involved Cornell Prescription Pharmacy, a small pharmacy in Colorado, which agreed to settle a complaint by OCR that alleged it disposed of unsecured documents containing the protected health information of "1,610 patients in an unlocked, open container on Cornell's premises."

The complaint further alleged that Cornell had no written policies or procedures as required under HIPAA, and had failed to train employees on privacy practices. The documents left out in the open (which contained identifiable patient information) were not shredded before disposal. The settlement requires Cornell to adopt and implement comprehensive privacy policies and practices, while complying with the Privacy Rule in the future.

HIPAA Privacy Rule: Learn It, Know It, Live It
The HIPAA Privacy Rule establishes requirements to protect individuals' medical records and other personal health information. It applies to health plans, healthcare clearinghouses, and those healthcare providers which conduct electronic healthcare transactions. Under recent HIPAA amendments, the rule extends downstream and also applies to business associates and even vendors of business associates.

The rule requires businesses to implement appropriate safeguards to protect the privacy of personal health information, including setting limits and conditions on the uses and disclosures of such information without patient authorization.

Costly Settlements Are Becoming The Norm

Cornell's recent settlement highlights a trend in HIPAA enforcement that began last year when two hospital systems paid $4.8 million to settle data breach claims. In that case, data from 6,800 individuals was compromised, including patient information, medications, vital statistic information, and lab results. The breach occurred when a physician attempted to deactivate a personal server, which resulted in data being released to the Internet in a searchable format.

Another recent enforcement action in the healthcare industry also resulted in a large settlement; a health system in Indiana had to pay an $800,000 settlement after one of its employees left 71 cardboard boxes of medical records unattended on the driveway of a physician's home.

Data breaches like these are a frequent source of HIPAA complaints according to Christine Heide, acting Deputy Director of Health Information Privacy at OCR. According to recent enforcement data, the most common issues investigated are: 1) impermissible uses and disclosures of protected health information; 2) lack of safeguards; 3) lack of patient access to protected health information; 4) lack of administrative safeguards of electronic protected health information; and 5) use or disclosure of more protected health information than is minimally reasonably needed.

Indeed, as these examples show, data breach and the resulting HIPAA implications will remain on the forefront of legal issues for entities in the healthcare industry for some time, especially where those entities fail to have proper policies and procedures compliant with HIPAA's Privacy Rule.

For more information, contact the author at NBeermann@fisherphillips.com or 206.693.5078.

Service Focus

Privacy and Cyber

Industry Focus

Healthcare