Health Information Compliance Alert

Case Study: Aetna Mail Breach Exposes PHI of Thousands of HIV Patients

Case highlights need for tighter internal protocols when delicate information is at stake.

Despite the best HIPAA-compliance efforts, healthcare organizations make mistakes. But sometimes, the breaches are so large and the fix so easy that outsiders wonder how such an error could happen.

Background: Large-scale HIPAA violations that expose electronic protected health information (ePHI) and violate the HIPAA Security Rule have dominated the news over the past year, garnering huge financial penalties. However, this past August saw a major mail snafu by a private payer that exposed the incredibly sensitive protected health information (PHI) of close to 12,000 individuals. Aetna Inc. sent HIV-specific information to 11,887 of its customers in 23 states in envelopes with large windows. Even a quick glance at the clear openings allowed any reader to see the HIV medical and drug details, which is a breach that falls under the HIPAA Privacy Rule for unauthorized disclosure.

"Aetna's actions are alleged to have violated federal and state privacy laws," said analysis of the case by the Philadelphia law firm **Berger & Montague, P.C.** on its website. "Aetna is accused of exposing people living with HIV to potential discrimination."

Look at the HIPAA violation on the OCR Breach Portal at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Disclosures Lead to Federal Class Action Suit Against Aetna

Though the OCR has yet to confer any penalty or make a statement about the HIPAA breach, one of Aetna's exposed customers has filed a class action suit against the private insurer, a Legal Action Center press release from Aug. 29 said.

"The lawsuit, filed today in U.S. District Court for the Eastern District of Pennsylvania, says information about HIV medication was clearly visible through the large window of the Aetna envelope, revealing the highly confidential matter to family, roommates, friends, neighbors, landlords, mail carriers, and even complete strangers," the release stated.

Past problems: A "stigma" still surrounds HIV, and surprisingly, Aetna's mailers were meant to be corrective measures to eradicate previous lawsuits regarding the privacy of its customers from 2014 and 2015, the release suggested.

"For 40 years, HIV-related public health messages have been geared toward assuring people that it's safe to come forward to get confidential HIV treatment, and now our clients come forward for HIV-related healthcare and Aetna fails to provide confidentiality," says **Ronda B. Goldfein**, executive director of the AIDS Law Project of Pennsylvania, which filed the suit along with the New York-based Legal Action Center and Berger & Montague, P.C. in Philadelphia.

"The lawsuit demands that Aetna cease the practice, reform procedures, and pay damages, including punitive damages," noted the Berger & Montague, P.C. online resources.

Consider this: An OCR penalty for a single disclosure of HIV-related information from a missent fax in 2014 by an employee at the Spencer Cox Center cost the organization $387,000 in fines this past May. That lost PHI "included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse," and was accidentally sent by fax to the patient's employer instead of to a P.O. box as requested, said an HHS-OCR release. (See Health Information Compliance Alert, Vol. 17, No. 6)

The verdict is still out on how the class action suit will turn out or whether more plaintiffs will join the fight against Aetna. But the OCR opinion on unauthorized disclosure, particularly of something as personal as health data related to HIV and

AIDS, is evident in both its past statements and penalties.

"Individuals cannot trust in a healthcare system that does not appropriately safeguard their most sensitive PHI," says **Roger Severino**, OCR director. "Covered entities and business associates have the responsibility under HIPAA to both identify and actually implement these safeguards."

He adds, "In exercising its enforcement authority, OCR takes into consideration aggravating factors such as the nature and extent of the harm caused by failure to comply with HIPAA requirements."

Resources: To read the Legal Action Center press release, visit https://lac.org/wp-content/uploads/2017/08/Aetna-Press-Release-8-28-17-Final.pdf.