HHS Settlement Shows: "You'd Better Implement

Digital Media and Data Privacy Law Blog

on 12.15.2014
Posted in Privacy

by Forrest Campbell, Health Law Attorney, fcampbell@brookspierce.com

In December 2014, the U.S. Department of Health and Human Services ("HHS") and Anchorage Community Mental Health Services ("ACMHS") settled alleged HIPAA violations for $150,000.

Don't be misled--this settlement is not important just for parties subject to HIPAA. It's important to anyone who maintains confidential information in electronic form.

Here's what happened according to HHS. ACMHS failed to regularly update its IT resources with available patches, and ACMHS used outdated, unsupported software. As a direct result of these two factors, malware was able to compromise the security of ACMHS's IT system, resulting in a data breach of the protected health information of 2,743 individuals. As HIPAA requires, ACMHS notified HHS of the breach, and an HHS investigation followed. The investigation led to the settlement. The period from the start of the investigation to the signing of the settlement was 2 ½ years--which probably represents a lot of hours and money for ACMHS.

These events show how important security patches and software updates are for all parties with confidential electronic information. If you fail to diligently implement patches and updates--no matter what business line you're in--malware might infiltrate your IT system and cause a data breach. Data breaches often require notice to the individuals affected and to state and federal authorities, and often lead to investigations, lawsuits, and/or settlements.

Apparently, ACMHS could have avoided the entire matter if it had implemented proper patches and updates.

Although the lessons from these events are important across all industries, parties subject to HIPAA should recall that the HIPAA security rule essentially mandates that critical security patches and updates be implemented. For example, the security rule broadly requires that HIPAA covered entities and business associates must:

- Ensure the confidentiality, integrity, and availability of all electronic PHI.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.

- Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under HIPAA.

HHS's Bulletin announcing and describing the settlement is located here:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf

The settlement is located here:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf

Forrest W. Campbell, Jr. practices in the Greensboro office of Brooks, Pierce, McLendon, Humphrey & Leonard, LLP. His practice is dedicated to health care. You are welcome to contact him at 336.373.8850 or fcampbell@brookspierce.com.