Health Law Alert: HIPAA Settlement Raises Questions about Malware Protection for Providers

February 13, 2015

Health Law Alert: HIPAA Settlement Raises Questions about Malware Protection for Providers

By Jesse Berg and Julia Marotte

Anchorage Community Mental Health Services (ACMHS) has agreed to settle with the Department of Health and Human Services' Office for Civil Rights (OCR) over potential HIPAA security violations. Due to malware, ACMHS experienced a breach of unsecured electronic protected health information (ePHI) that affected 2,743 individuals. The settlement sheds light on OCR's reaction to HIPAA breaches resulting from malware and reinforces the importance of developing and enforcing a thorough HIPAA compliance plan. It also reminds providers of the importance of periodically reviewing their software protections. In light of the growing risks in today's heavily regulated world and increasing volumes of electronic information flowing every which way, providers should consider the importance of whether updates are needed.

ACMHS' Malware Incident

ACMHS is a community-based, nonprofit organization that provides behavioral health care services to children, adults, and families in Anchorage, Alaska. In 2012, ACMHS self-reported a breach of ePHI that resulted from malware compromising the security of ACMHS' information technology resources. OCR initiated an investigation, which revealed that ACMHS was not adequately complying with HIPAA Privacy, Security, and Breach Notification Rules. According to OCR, ACMHS' security measures were deficient in numerous respects. OCR noted that ACMHS adopted HIPAA security rule policies and procedures in 2005, but did not follow these rules. In addition, OCR stated that ACMHS failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI and failed to implement technical security measures to protect against unauthorized access to ePHI. OCR concluded, "[t]he security incident was a direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software."

Under the Resolution Agreement, ACMHS is required to pay $150,000, comply with a corrective action plan, and report on the state of its compliance to OCR for two years. The corrective action plan requires ACMHS to take steps to improve its HIPAA compliance program, including revising and adopting new security rule policies and procedures, training workforce members on its security rule policies and procedures as well as general security awareness, and assessing security risks to the confidentiality, integrity, and availability of ePHI on an annual basis.

Managing the Threat of Malware

The volume and sophistication of today's cyber threats makes malware an issue of particular concern. While organizations must be vigilant in protecting against malware or other data breaches, simple daily actions can go a long way. Organizations should frequently review their systems to make sure they are up to date and running properly. According to OCR Director Jocelyn Samuels, "Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis. This includes reviewing systems on unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."

With that said, having and enforcing an effective compliance plan is critical. Organizations must develop security measures sufficient to reduce risks and vulnerabilities to ePHI. In addition, organizations must ensure their workforce receives regular training on security measures. Employees should understand the importance of guarding against, detecting, and reporting malicious software. Perhaps the only thing more important than compliance plan development and training is compliance plan enforcement. OCR was quick to note that ACMHS had a compliance plan in place, but failed to enforce it. In addition, like many past HIPAA settlements, the ACMHS matter highlights the dangers associated with simply adopting "off the shelf" HIPAA policies and procedures, while failing to actually implement those materials into the organization's compliance infrastructure or train personnel related to compliance. Further, all regulated parties should remember that as technology develops and grows, their obligations to adopt—or at least consider adopting — updates likewise will increase.

View the Resolution Agreement online here at the U.S. Department of Health & Human Services.

If you have questions regarding the ACMHS settlement or HIPAA compliance generally, please contact Jesse Berg at jesse.berg@lathropgpm.com (612.632.3374) or Julia Marotte at julia.marotte@lathropgpm.com (612.632.3280).