THE
NATIONAL LAW REVIEW

Just in Time for the Holidays: Another HIPAA Settlement

McDermott Will & Emery

Article By
Edward G. Zacharias
McDermott Will & Emery
Publications - Insights

- Civil Rights
- Health Law & Managed Care
- Communications, Media & Internet
- Litigation / Trial Practice

- Alaska

Thursday, December 11, 2014

On December 2, 2014, **the Office for Civil Rights (OCR) and Anchorage Community Mental Health Services, Inc.**, (ACMHS) entered into a **Resolution Agreement and Corrective Action Plan (CAP) to settle alleged violations of the HIPAA Security Rule**, which governs the safeguarding of electronic protected health information (ePHI). OCR initiated an investigation into ACMHS's compliance with HIPAA after receiving a March 2, 2012 notification from the provider regarding a breach of unsecured ePHI affecting 2,743 individuals. The breach resulted from malware that compromised ACMHS's information technology resources.

OCR's investigation found that ACMHS (1) had never performed an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by ACMHS; (2) had never implemented Security Rule policies and procedures; and (3) since 2008, had failed to implement technical security measures to guard against unauthorized access to ePHI transmitted electronically, by failing to ensure that appropriate firewalls were in place and regularly updated with available patches.

ACMHS agreed to pay $150,000 and to comply with the requirements set forth in the CAP to settle the allegations. The CAP has a two-year term and obligates ACMHS to take the following actions:

- Revise, adopt and distribute to its workforce updated Security Rule policies and procedures that have been approved by OCR
- Develop and provide updated security awareness training (based on training materials approved by OCR) to applicable workforce members, and update and repeat the training annually
- Conduct annual risk assessments of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by ACMHS, and document the security measures implemented to reduce the risks and vulnerabilities to a reasonable and appropriate level
- Investigate and report to OCR any violations of its Security Rule policies and procedures by workforce members
- Submit annual reports to OCR describing ACMHS's compliance with the CAP

In announcing the settlement, OCR Director Jocelyn Samuels said, "[s]uccessful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis. This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks." A copy of the Resolution Agreement and CAP can be found here.

The settlement is another reminder that covered entities and business associates should ensure that they have taken steps necessary and appropriate to safeguard the ePHI in their possession. Conducting regular ePHI risk assessments, addressing any identified security vulnerabilities, implementing and updating comprehensive HIPAA policies and procedures, and appropriately training workforce members who have access to ePHI are all steps that covered entities and business associates must take to comply with HIPAA and protect ePHI.