

December 2014
U.S. Department of Health and Human Services
Office for Civil Rights

BULLETIN: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software

Anchorage Community Mental Health Services (ACMHS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with the Department of Health and Human Services (HHS), Office for Civil Rights (OCR). ACMHS will pay \$150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. ACMHS is a five-facility, nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.

OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to malware compromising the security of its information technology resources. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the 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identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

“Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis,” said OCR Director Jocelyn Samuels. “This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks.”

ACMHS cooperated with OCR throughout its investigation and has been responsive to technical assistance provided to date. In addition to the \$150,000 settlement amount, the agreement includes a corrective action plan and requires ACMHS to report on the state of its compliance to OCR for a two-year period. The Resolution Agreement can be found on the OCR website at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

The HHS Office for Civil Rights and Office of the National Coordinator for Health Information Technology offer a Security Rule Risk Assessment Tool to assist organizations that handle protected health information in conducting a regular review of the administrative, physical and technical safeguards they have in place to protect the security of the information. The tool is available at: <http://www.healthit.gov/providers-professionals/security-risk-assessment>

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on how to file a complaint, visit us at <http://www.HHS.gov/OCR>

Follow us on Twitter @HHSOCR.

###