# PUBLICATION

## HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software

**Authors: Alisa L. Chestler**
**December 10, 2014**

The title of this alert, which comes straight from the Department of Health and Human Services Office for Civil Rights' (OCR) announcement of its most recent settlement, again underscores the critical need for covered entities and business associates to undertake a thorough security risk analysis. On December 8, 2014, OCR announced a settlement with Anchorage Community Mental Health Services (ACMHS), a five facility, non-profit organization providing behavioral health care services in Anchorage, Alaska, for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). OCR opened an investigation after ACMHS notified the agency of a breach of unsecured electronic protected health information (ePHI) due to malware found on a desktop computer between December 20, 2011 and January 4, 2012. As a result of this breach, which affected over 2,500 individuals, ACMHS will pay $150,000 and adopt a corrective action plan (CAP) to correct deficiencies in its HIPAA compliance program. ACMHS will also be required to report on the state of its HIPAA compliance to OCR for a two-year period.

Once again, OCR's investigation found a covered entity that had not taken the time to update its policies and procedures to stay in line with current standards or expectations. While ACMHS adopted sample Security Rule policies and procedures in 2005, such policies and procedures were not followed. OCR's findings included a determination that the breach was the direct result of ACMHS's failure to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

It is significant to point out that the resolution agreement focused on ACMHS' failure to conduct an accurate and thorough security risk analysis as required by the Security Rule. We recommend that all covered entities and business associates revisit their most recent security risk analysis and ensure that the issues associated with patch management are addressed. It seems clear that OCR will continue to expect all entities that handle ePHI to meet these requirements, regardless of an entity's size, mission or non-profit status.

This settlement should also serve as a reminder that the HIPAA audit program will be resuming after the first of the year. Accordingly, hundreds of covered entities and business associates will be receiving inquiries that could lead to an onsite audit. The audit requirements will be onerous and very difficult for organizations that have not planned in advance for such an event. We are currently assisting clients with mock audits and updates to their HIPAA compliance programs and will be happy to discuss the challenges presented by these reviews. As demonstrated again by OCR's most recent resolution agreement, the risks of non-compliance simply outweigh the costs of sound preparation.

If your business needs help with its privacy or data security procedures and practices, or if you have questions about this Alert or any other federal or state privacy laws, please contact your Baker Donelson attorney.