eALERT

INCompliance

December 15, 2014

Don't Let This Be You: Provider Agrees to a $150,000 HIPAA Settlement in Potential Security Breach Matter

Have you conducted a HIPAA security risk assessment? If so, do you review the results of that assessment and determine whether it needs to be updated periodically? Failure to conduct initial and periodic HIPAA security risk assessments is one of the biggest reasons covered entities are assessed fines and penalties by the Department of Health and Human Services (HHS).

It was recently announced that Anchorage Community Mental Health Services (ACMHS) has agreed to pay $150,000 to the HHS Office of Civil Rights (OCR) in settlement of potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The potential breach occurred when unsecured electronic protected health information (ePHI) affecting 2,743 individuals was compromised by malware that had infected ACMHS's information technology resources.

Although ACMHS had adopted sample Security Rule policies and procedures in 2005, it had not been following the procedures and as a result failed to identify and address basic risks, such as not regularly updating their information technology resources with available patches and running outdated, unsupported software. In OCR's press release, OCR Director Jocelyn Samuels warned providers that successful HIPAA compliance requires a regular risk assessment that "includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."

In addition to the monetary settlement, ACMHS has also agreed to adopt a corrective action plan to address deficiencies in its compliance program, which includes conducting a risk assessment, adopting revised policies and procedures and workforce training.

Rapidly changing technology is creating new challenges to assuring ePHI security. By conducting a regular risk assessment, ACMHS may have been able to identify the risks and avoid the penalty in this case. In order to be in full compliance with the Security Rule, it is essential that health care providers monitor compliance and audit their security program, including conducting periodic security risk assessments and updating their policies and procedures to address new technology and organizational changes.

This joint INCompliance and Bricker & Eckler E-Alert was prepared by Joshua M. Gilbert and Elisabeth A. Squeglia. They can be reached at esqueglia@incomplianceconsulting.com or jgilbert@bricker.com. Please contact Josh or Bette, or any member of the INCompliance consulting staff or the Bricker & Eckler Health Care Group for more information about legal and consulting HIPAA compliance services.