September 25, 2012

Another Costly HIPAA Breach

The U.S. Department of Health and Human Services ("HHS") continued its aggressive HIPAA enforcement activity in September. Like many recent enforcement actions, this new one was the result of a breach of ePHI, which was reported to HHS and triggered an investigation into whether the covered entity was in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule and Security Rules ("Privacy and Security Rules").

On September 17, HHS announced that the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates (collectively, "Massachusetts Eye & Ear") agreed to pay a **$1.5 million** fine and entered into a Resolution Agreement and Corrective Action Plan ("CAP"). As required under the HITECH Act, the Massachusetts Eye & Ear reported a breach of unsecured electronic protected health information (ePHI) to HHS on April 21, 2010. The breach occurred when a laptop was stolen which contained unencrypted ePHI of more than 3,600 Massachusetts Eye & Ear patients and research subjects. On October 5, 2010, HHS notified Massachusetts Eye & Ear that it was investigating its compliance with the Privacy and Security Rules, as well as the Breach Notification Rule.

HHS concluded that the Massachusetts Eye & Ear failed to comply with the HIPAA Privacy and Security Rules in several respects, including:

- Massachusetts Eye & Ear's security measures were insufficient to protect ePHI on portable devices.

- Massachusetts Eye & Ear failed to adopt or implement policies and procedures to address security incident reporting, maintain awareness of what type of portable devices were being used to access its network.

- Massachusetts Eye & Ear did not document a rationale supporting the decision not to encrypt ePHI on portable devices, nor did it implement an equivalent, reasonable, and appropriate alternative to encryption.

In addition to the fine of $1.5 million dollars, Massachusetts Eye & Ear faces other costly and time consuming requirements as a result of the breach. For example, HHS also required Massachusetts Eye & Ear to agree to a detailed CAP which includes the following requirements:

- Massachusetts Eye & Ear must adopt policies and procedures to comply with the HIPAA Privacy and Security Rules, including procedures to track the receipt and removal of hardware and electronic media, including portable devices, which contain ePHI into, out of, and within its facilities, and mechanisms to encrypt and decrypt portable devices containing ePHI.

- Massachusetts Eye & Ear must train all workforce members on the policies and procedures, and sign a certification that they have received training.

- Massachusetts Eye & Ear must submit a written report on its implementation of the CAP within 120 days after HHS has approved its policies and procedures, including copies of all training materials and signed attestations.

- Massachusetts Eye & Ear must engage an independent monitor acceptable to HHS who will monitor compliance in accordance with a monitoring plan approved by HHS.

The size of the fines and the extent of the CAP requirements in this settlement are high given the number of individuals' records involved. Covered entities should take notice of this settlement as it likely marks a trend of more aggressive HIPAA breach enforcement by HHS.

Has your organization reviewed your HIPAA policies and procedures to make sure they adequately address the security of ePHI on portable and mobile devices? Nearly all of the recent enforcement actions resulting in 7 figure penalties have been the result of breaches within organizations that HHS determined had inadequate policies and procedures to protect the security of ePHI. Many involved portable and mobile devices.

Today's world sometimes seems to revolve around portable and mobile electronic devices, and few people don't have one they use daily. But the risk of allowing your employees to use portable and mobile devices to store or access ePHI is extremely high. It is sometimes difficult to prohibit the use of laptop computers, iPhones, iPads, blackberries and other portable and mobile devices by employees, but there are precautions you can take to make sure you avoid the type of penalty imposed on Massachusetts Eye & Ear.

If you haven't reviewed your HIPAA compliance program to make sure it is up to date and fully in compliance with the Privacy and Security Rules, an audit may be in order, to make sure the next enforcement action is not against you.

This E-Mail Alert was prepared by Bryn Hunt and Bette Squeglia. Please contact any INCompliance consultant for more information. This and previous E-Mail Alerts may be accessed on our E-Mail alert webpage.