eALERT

INCompliance

February 13, 2017

Are your HIPAA practices in sync with today's technology? Three notable HIPAA enforcement actions in 2017

When was the last time you thoroughly reviewed your operations to make sure your HIPAA compliance program has been fully implemented and is effective?

Recent enforcement actions by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), highlight the importance of periodically reviewing the implementation of your written HIPAA policies to make sure the procedures you are following address risks inherent in today's rapidly changing technology. Many covered entities periodically review their written policies, but neglect to take the next step of determining whether the policies are being applied to all aspects of their operations and are effective. Periodic operational audits or risk assessments, and periodic retraining of your staff, will go a long way toward effectively monitoring and managing risk.

OCR has continued to increase enforcement activity, imposting significant fines when covered entities fail to monitor risk and act promptly to remediate it, as evidenced in the three recent enforcement actions discussed below.

Unencrypted electronic protected health information (ePHI) on mobile devices – Children's Medical Center of Dallas

OCR levied a civil money penalty of $3.2 million against Children's Medical Center of Dallas based on its impermissible disclosure of unsecured ePHI and noncompliance over many years with multiple standards of the HIPAA Security Rule.

The issues stemmed from the loss of an unencrypted BlackBerry device containing ePHI of approximately 3,800 individuals in 2009 and the theft of an unencrypted laptop from its premises containing the ePHI of 2,462 individuals in 2013, both of which were reported as breaches by the hospital. OCR's investigation revealed that the hospital had failed to implement risk management plans, contrary to prior external recommendations to do so, and failed to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April 9, 2013.

(Information from OCR, including the press release and Notice of Final Determination, is available here.)

Takeaway: If a covered entity allows ePHI on unencrypted mobile devices, it is inviting trouble. Loss/theft of mobile devices is inevitable and covered entities should understand the security risks that must be addressed, ideally by encryption rendering the ePHI secured.

Failure to act on known risks – MAPFRE Life Insurance Company of Puerto Rico

MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) underwrites and administers a variety of insurance products and services in Puerto Rico, including personal and group health insurance plans. MAPFRE entered into a settlement with OCR to resolve potential noncompliance with the HIPAA Privacy and Security Rules related to the theft of an unencrypted USB data storage device by paying $2.2 million and implementing a corrective action plan.

In 2011, MAPFRE filed a breach report acknowledging theft of a USB data storage device containing the ePHI of 2,209 individuals. OCR determined that MAPFRE had failed to conduct its risk analysis and implement risk management plans, contrary to its prior representations, and had failed to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014. The delay in implementing corrective measures was specifically noted by OCR, with Director Samuels stating, "[c]overed entities must not only make assessments to safeguard ePHI, they must act on those assessments as well."

(Information from OCR, including the Resolution Agreement and Corrective Action Plan, is available here.)

Takeaway: Again, ePHI being stored on unencrypted mobile devices/media resulted in large penalties. Additionally, covered entities must act on the risk assessments they conduct. Failure to address known risks will likely result in violations and significant penalties.

Failure to make timely breach notification – Presence Health

In the first HIPAA settlement based on the untimely reporting of a breach of unsecured PHI, Presence Health agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and implementing a corrective action plan.

On October 22, 2013, Presence Health discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from one of its surgery centers. Presence Health did not report the breach to OCR until January 31, 2014, well outside of the requirement to report without unreasonable delay and no later than 60 days after discovery of the breach. The resolution agreement states that Presence Health reported that the delay was due to miscommunication between its workforce members.

OCR's investigation indicated that Presence Health failed not only to report the breach to OCR in a timely manner but also to report the breach to the media and to notify the individuals affected within the timeframes required. Additionally, the resolution agreement indicates that OCR found additional instances of breaches affecting fewer than 500 individuals reported in 2015 and 2016 in which the individuals affected were not notified in a timely manner.

OCR noted that in reaching the settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire to not disincentivize reporting of breaches altogether.

(Information from OCR, including the Resolution Agreement and Corrective Action Plan, is available here.)

Takeaway: Prompt investigation and assessment is critical when a possible breach of unsecured PHI is suspected. The time period for notifying individuals affected, in all cases, is without unreasonable delay and no later than 60 days after discovery of the breach. Reporting to HHS and the media is required no later than 60 days after discovery for breaches affecting 500 or more individuals. Reporting to HHS for breaches affecting less than 500 individuals is required within 60 days of the end of the calendar year in which the breach occurred (e.g., by March 1, 2017, for breaches in 2016).

INCompliance offers a wide array of customized audit and risk assessment services to help you stay in compliance and avoid costly investigations and penalties. Contact one of our HIPAA consultants or email us today at info@incomplianceconsulting.com about an effectiveness audit of your HIPAA compliance program or a risk assessment and training.

Our attorney consultants include:
Chris Bennington, cbennington@incomplianceconsulting.com, 513.870.6572
Allen Killworth, akillworth@incomplianceconsulting.com, 614.227.2334
Bette Squeglia, esqueglia@incomplianceconsulting.com, 614.227.2396

This Alert was prepared by Allen Killworth and Bette Squeglia. For more information about INCompliance and our services, go to www.incomplianceconsulting.com.