eALERT

INCompliance

June 16, 2014

HHS Reports HIPAA Breaches Increased Substantially and Predicts More Enforcement in 2014

The Department of Health and Human Services (HHS) released two reports to Congress as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act: a breach report, Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2011-2012 and a compliance report, Annual Report to Congress on HIPAA Privacy, Security and Breach Notification Rule Compliance for Calendar Years 2011-2012.

The breach report details the number and nature of breaches reported to HHS and the actions taken in response to those breaches. Much of this information has already been made available publicly by HHS on its Breach Notification webpage. A few notable statistics from the breach report are:

- Health care providers continue to be the entities with the most total number of breaches: 63 percent of all breaches in 2011 and 68 percent of all breaches in 2012. However, business associates are responsible for a large portion of the number of individuals affected by breaches because despite the fact that business associates as a category have fewer breaches, their breaches affect more individuals. In 2011, of all the individuals affected by breaches, 64 percent were affected by breaches made by business associates and in 2012, 42 percent were affected by breaches made by business associates.
- Theft of protected health information (PHI) remains the most significant cause of breaches; 50 percent of breaches in 2011 and 53 percent of breaches in 2012 were caused by theft.
- Laptops and portable devices represent the largest source of PHI breaches; 33 percent of breaches in 2011 and 36 percent of breaches in 2012 were from PHI on laptops or other portable electronic devices.
- Small breaches, those affecting fewer than 500 individuals, dramatically increased in 2011-2012 from the two years prior – or at least the reporting of those small breaches has increased. Small breaches reported over the past four years total: 12,000 in 2009, 50,000 in 2010, 151,605 in 2011 and 165,135 in 2012.
- However, the breach report notes that from 2011-2012 large breaches, those affecting 500 or more individuals, made up only 0.97 percent of reports (458 reports affecting 500 or more individuals out of 47,357 total reports), yet accounted for 97.89 percent of the 15,005,660 individuals affected by a PHI breach.

The breach report contains a section on "lessons learned" and states that these are "areas to which covered entities should pay particular attention in their compliance efforts to help avoid some of the more common types of breaches." There are no surprises in the lessons learned. Expectedly, the recommendations from the breach report are:

- **Risk Analysis and Risk Management.** Ensure the organization's security risk analysis and risk management plan are thorough, having identified and addressed the potential risks and vulnerabilities to all electronic protected health information (ePHI) in the environment, regardless of location or media. For example, this includes ePHI on computer hard drives, digital copiers and other equipment with hard drives, USB drives, laptop computers, mobile phones and other portable devices, and ePHI transmitted across networks.
- **Security Evaluation.** Conduct a security evaluation when there are operational changes, such as facility or office moves or renovations, that could affect the security of PHI and ensure that appropriate physical and technical safeguards remain in place during the changes to protect the information when stored or when in transit from one location to another. In addition, conduct appropriate technical evaluations where there are technical upgrades for software, hardware, and websites or other changes to information systems to ensure PHI will not be at risk when the changes are implemented.
- **Security and Control of Portable Electronic Devices.** Ensure PHI stored and transported on portable electronic devices is properly safeguarded, including through encryption where appropriate. Have clear policies and procedures that govern the receipt and removal of portable electronic devices and media containing PHI from a facility and provide how such devices and the information on them should be secured when off-site.
- **Proper Disposal.** Implement clear policies and procedures for the proper disposal of PHI in all forms. For electronic devices and equipment that store PHI, ensure the device or equipment is purged or wiped thoroughly before it is recycled, discarded or transferred to a third party, such as a leasing agent.
- **Physical Access Controls.** Ensure physical safeguards are in place to limit access to facilities and workstations that maintain PHI.
- **Training.** Ensure employees are trained on the organization's privacy and security policies and procedures, including the appropriate uses and disclosures of PHI and the safeguards that should be implemented to protect the information from improper uses and disclosures; and ensure employees are aware of the sanctions and other consequences for failure to follow the organization's policies and procedures.

The compliance report details complaint and enforcement data including, with respect to complaints received and compliance reviews begun during the years 2011-2012:

1. The number of complaints;
2. The number of complaints resolved informally, including a summary of the types of such complaints;

3. The number of complaints that resulted in the imposition of civil money penalties or have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement;
4. The number of compliance reviews conducted and the outcome of each such review; and
5. The number of subpoenas or inquiries issued.

The compliance report also provides a summary of significant activities including resolution agreements, civil monetary penalties and subpoenas. Much of this information has already been made available publicly by HHS on its HIPAA Enforcement webpage.

It was also reported separately that HHS Chief Regional Civil Rights Counsel Jerome Meites stated at a recent American Bar Association conference that penalties under HIPAA would likely increase substantially in the next year. While it is not clear exactly what this signals, covered entities and business associates should take note that HHS may be moving towards even greater enforcement in the HIPAA area.

Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com. This E-Alert may also be accessed on the INCompliance website.