HIPAA Privacy & Security Updates—From Dorothy Cociu, COIN Editor and HIPAA Privacy & Security Consultant & Trainer

There is an important deadline of March 1 for any Covered Entity or Business Associates (like agents) who had HIPAA Privacy & Security Small Breaches in 2016. On March 1, 2017: HIPAA Privacy Data Breach filings for 2016 are due to HHS. If you or one of your clients had one or more data breaches in 2016 that affected 500 or fewer individuals, you must notify HHS/OCR within 60 days of the end of 2016 of the breach; ie March 1. You may report earlier, but if you have not, you must do so by March 1. Even if you filed with the state (ie certain providers, etc.), you must still file the federal filings by March 1. If the breach affected 500 or more individuals, you are required to report without reasonable delay, but no later than 60 days after the discovery, so those filings may be past due.

Breach reports must be submitted online via OCR's breach portal. The breach portal requires a separate fillable report for each breach.

If you have questions, you can call HHS OCR toll-free at 800-368-1019, or email OCRPrivacy@hhs.gov.

Enforcement Updates

Several enforcement actions have been reported by HHS/OCR since the last issue of the COIN was released.

On January 10, 2017, OCR announced 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 agreeing to implement a corrective action plan. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long term care and senior living facilities, as well as physicians offices and health care centers., and offers home care, hospice care, and behavioral health services.

On January 18, 2018, HHS/OCR announced a HIPAA settlement based on impermissible disclosure of unsecured electronic PHI. MAPFRE Life Insurance Company agreed to settle paying **$2.2 Million** and implement a corrective action plan. MAPFRE underwrites and administers a variety of Insurance products and services in Puerto Rico, including personal and group health insurance plans. In 2011, they filed a breach report with OCR indicating that a USB data storage device containing ePHI was stolen from it's IT department where it was left overnight. The device contained names, dates of birth and social security numbers. The breach affected 2,209 individuals. OCR's investigation revealed MAPFRE's noncompliance with the HIPAA rules, specifically, a failure to conduct its risk analysis and implement risk management plans, and a failure to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September, 2014. They also failed to implement or delayed implementing other corrective measures it informed OCR that it would undertake.

February 1, 2017, HHS/OCR reported a lack of timely action risks security and costs money, when announcing a **HIPAA Civil Monetary Penalty in the amount of $3.2 million** against Children's Medical Center of Dallas (Children's) based on an impermissible disclosure of ePHI and noncompliance over many years with multiple standards of the HIPAA Security Rule. The Civil Monetary Penalty follows a breach report filed in 2010, indicating the loss of an unencrypted, non-password protected Blackberry Device at Dallas/Fort Worth International Airport in 2009, which contained the electronic PHI of approximately 3,800 individuals. In 2013, a separate breach report was filed, reporting the theft of an unencrypted laptop from its premises, which included the ePHI of 2,462

individuals.

The investigation revealed that Children's noncompliance with the HIPAA rules, specifically, a failure to implement risk management plans, contrary to prior external recommendations to do so, and failure to deploy encryption or an equivalent alternative measure, on all of its devices and workstations, mobile devices and removable storage data, until April, 2013. (This is an example of "Willful Neglect" in privacy training).

Lastly for this issue, on February 17, 2017, Memorial Healthcare Systems (MHS) paid a **$5.5 million HIPAA settlement** to settle potential violations of the HIPAA Privacy & Security Rules, and agreed to implement a robust corrective action plan.

MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout South Florida.

MHS reported to HHS/OCR that PHI of 115,143 individuals had been impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. *The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained on a daily basis without detection for a period of a year, affecting 80,000 individuals.* Although they had policies and procedures in place, they failed to terminate former employees' right to access, as required by the HIPAA rules. Further, they failed to regularly review records of information system activity on applications that maintain electronic PHI by workforce users at affiliated physician practices, despite having identified the risk on several risk analyses conducted by MHS.

More updates will appear in the next issue of the COIN. ##