HIPAA Privacy & Security Updates—November, 2017

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

So what's happened with HIPAA Privacy & Security Enforcement and updates since the September issue? As usual, quite a few things.

On October 13, 2016, St. Joseph Health (SJH) agreed to settle potential privacy violations following a report that ePHI were publicly accessible through internet search engines from 2011-2012. 14 acute care hospitals, home health care agencies, hospice care, outpatient services, SNF, community clinics and physician organizations throughout CA, parts of Texas and New Mexico. SJH agreed to pay **$2.14 million settlement** and adopt a comprehensive corrective action plan after a 2/14/12 report filed with HHS/OCR that certain files it created for its participation in the meaningful use program, which contained ePHI, were publicly accessible on the internet from February 1, 2011 through February 13, 2012, via Google and possibly other internet search engines. **The server SJH purchased to store files included a file sharing application whose default settings allowed anyone with an internet connection to access them**, resulting in unrestricted access to PDF files containing ePHi of 31,800 individuals, including patient names, health statuses, diagnosis, and demographic information.

The OCR Investigation indicated that SJH potential violations included failure to conduct an evaluation in response to operational changes presented by implementing a new server, therefore compromising ePHI; contractors hired to assess the risks and vulnerabilities were done in a patchwork fashion and did not result in an enterprise-wide risk analysis. In addition to the $2.14 million settlement, they must comply with a corrective action plan that requires the organization to conduct an enterprise-wide risk analysis, develop and implement a risk management plan, revise its policies and procedures, and train its staff on these policies and procedures.

On September 23, 2016, HHS Office of Civil Rights released information on a HIPAA settlement which illustrates, again, the importance of reviewing and updating, as necessary, Business Associates Agreements. Care New England Health System (CNE), on behalf of each of the covered entities under its of HIPAA Privacy & Security Rules. The settlement includes a monetary penalty of $400,000 and a comprehensive corrective action plan. CNE provides centralized corporate support for its subsidiary affiliated covered entities, including but not limited to finance, HR, IT and technical support, insurance, compliance and administrative functions.

In November, 2012, HHS and OCR received notification from Woman & Infants Hospital of Rhode Island (WIH), a covered entity member of CNE, of the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient names, DOB, date of exam, physician names, and in some cases, social security numbers. As WIH's business associate, CNE provides centralized corporate support including IT services and support for WIH's systems. *The BA Agreement was effective March 15, 2005, and was not updated until August 28, 2015, as a result of the OCR investigation, and therefore, did not incorporate revisions required under the HIPAA Omnibus Final Rule.*

The investigation found that for almost a year, WIH disclosed PHI and allowed its business associate, CNE, to create, receive, maintain, or transmit PHI on its behalf, without obtaining satisfactory assurances as required under HIPAA. ***WIH failed to renew or modify its existing written BA Agreement with CNE to include the applicable implementation specifications required by HIPAA***. During that same time-period, WIH impermissibly disclosed PHI of at least 14,000 individuals to its business associate when WIH provided CNE with access to PHI without obtaining satisfactory assurances, in the form of a written BA agreement, that CNE would appropriately safeguard the PHI.

With respect to the underlying breach, WIH entered into a consent judgement with the Massachusetts Attorney General's Office, and reached a settlement of $150,000. OCR found the consent judgement to sufficiently cover most of the conduct in this breach, including the failure to implement appropriate safeguards related to the handling of backup tapes and the failure to provide timely notification to the affected individuals.

Note that the $150,000 penalty/settlement for WIH is in addition to the $400,000 penalty/settlement with CNE.

In other HIPAA News, On October 13, 2016, HHS/OCR released Health Information in the Digital Age; Where to Focus Enforcement Efforts. In this release, OCR restated its commitment to protecting health information in the digital world, including Social Media applications, mobile device security, and the tools needed to protect risk to privacy and security of this information. In the past 2 years, OCR has released extensive guidance on a host of HIPAA issues, as well as created a portal to provide technical assistance to those developing new technologies.

At the same time, OCR continues to maintain a robust enforcement program to hold entities accountable when compliance issues arise. They initiated Phase II of their Audit Program, which they feel will help to "correct problems before they ripen into HIPAA violations."

OCR continues to review every complaint filed received from the public.

On October 7, 2016, HHS/OCR released Cloud Computing Guidance, which is available at http://www.hhs.gov/hipaa/for-professionals/special-tpics/cloud-computing/index.html .

HHS also released on October 17, 2016, Resources for Mobil Health Apps Developers. This includes interactive tools, a developer portal, and a platform to ask questions about HIPAA Privacy & Security.

I will update you more next issue!

##