SANDBERG PHOENIX

PHYSICIAN LAW BLOG

Sidestepping Encryption? Better Be Ready To Pay Millions for HIPAA Violations

AUTHOR: DIANE ROBBEN, KEVIN PEEK

Earlier this week, the University of Texas MD Anderson Cancer Center was ordered to pay a staggering $4,348,000.00 in order to resolve HIPAA violations from data breaches occurring in 2011, 2012, and 2013. The extremity of the penalties is explained by the fact that the data breaches were completely preventable.

Generally, covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA) are required to ensure confidentiality, integrity, and availability of all electronic protected health information (ePHI) that is created, received, maintained, or transmitted, and protect that information from reasonably anticipated threats and impermissible uses. 45 C.F.R. § 164.306(a).

Surprisingly, the MD Anderson data breaches were not caused by the malicious intents of a rogue employee or someone internally with an insidious agenda. Rather, it began with three separate accidents off campus: the theft of a laptop computer from the home of a MD Anderson employee, and the loss of two USB thumb drives. Each of these devices contained ePHI of thousands of patients. None of the devices were encrypted.

Allowing the plot to thicken further, many years prior to these thefts and accidents, MD Anderson conducted a series of risk analyses as required under HIPAA. In doing so, it was revealed that there was a serious threat to the safety, security, and confidentiality of the ePHI on unencrypted devices used by employees. Seeming ahead of the game, MD Anderson developed policies in 2006 that required any portable device associated with MD Anderson to be encrypted. Sadly, these policies were only paid partial lip service as MD Anderson still did not have the encryption process complete by the time the last of the aforementioned devices was lost in 2013.

The U.S. Department of Health and Human Services (HSS) Office for Civil Rights (OCR), the enforcer of HIPAA, determined that there was a violation or two. MD Anderson disagreed on this finding by indicating that the data on its devices were used for research purposes, and that they were not subject to HIPAA's nondisclosure requirements. Obviously, OCR was not swayed by such a weak argument.

A case was filed and all arguments lead to the above mentioned final decision issued by the Administrative Law Judge. The below is an important excerpt to the reasoning behind the judge's decision:

[MD Anderson] is a comprehensive cancer center that operates both inpatient and outpatient facilities in the Houston, Texas area, was not only aware of the need to encrypt devices in order to assure that confidential data including ePHI not be improperly disclosed, but it established a policy requiring the encryption and protection of devices containing ePHI. However, and despite this awareness and its own policies, [MD Anderson] made only half-hearted and incomplete efforts at encryption over the ensuing years.

To remedy MD Anderson's noncompliance with 45 C.F.R. § 164.312 (a) (Technical Safeguards; encryption), the judge ordered a civil money penalty of $2,000 per day for each day from March 24, 2011, through January 25, 2013. To remedy Anderson's noncompliance with 45 C.F.R. § 164.502 (a) (Uses and Disclosure of PHI; impermissible disclosure of ePHI), the judge ordered a civil money penalty of $1,500,000 per year for the years 2012 and 2013.

While the final penalty amount looks fairly substantial on paper, the judge points out the following:

Penalties of $2,000 are only 1/25th of the maximum allowable amount for daily penalties. The annual penalties of $1,500,000 appear to be large but come to less than $90 for each violation committed by Respondent. The reality is that the penalties in this case are quite modest given the gravity of Respondent's noncompliance.

The number of employees working remotely has steadily increased in the past decade in a majority of white collar fields with no signs of slowing down. For those working with confidential information, and especially those in the healthcare fields working with private health information, data encryption is key. Not only is it a matter of responsibility, but it will help to avoid such debilitating fines as that suffered by MD Anderson. HIPAA was put in place for the benefit of everyone, but if misunderstood, can seem like a financial pain to those trying to keep up. Not only must covered entities and business associates implement robust privacy and security policies, but following and enforcing them is critical. Stay up to date with the latest HIPAA news and perform regular Risk Analyses to avoid an MD Anderson debacle.