SQUIRE PATTON BOGGS

How to Avoid Paying US$2,000 a Day to Encrypt Data

Let us hope you do not pay that much to encrypt electronic data. How about a total of US$4.3 million over two years? Well, that is the total penalty for encryption and unauthorized PHI disclosure violations assessed by Health and Human Services (HHS). An administrative law judge found the penalty could have been much worse. The facts are sobering. The message is clear.

Two Failures

In this case, a cancer center in Texas failed to encrypt electronic Protected Health Information (ePHI) for nearly two years, between 2011 and 2013. In 2012, an unencrypted laptop without password protection was stolen that contained the ePHI of almost 30,000 individuals. The ePHI included names, social security numbers and treatment or research information. In 2012, an unencrypted USB drive was lost that contained the same kind of ePHI of more than 2,200 individuals. In 2013, an unencrypted USB was lost that was believed to contain similar ePHI of approximately 3,600 individuals.

HHS imposed penalties and the center appealed to an administrative law judge. The judge found two violations of the requirement to protect ePHI created by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The center failed to limit access of ePHI to authorized individuals in violation of 45 C.F.R. § 164.312(a). Through theft and loss, the center also disclosed ePHI in violation of 45 C.F.R. § 164.502(a).

The Sobering Facts

In 2006, the center's security operations manual required that laptops be encrypted or protected with access controls. The manual also required that data on transportable media be encrypted. This policy was reiterated in subsequent documents. In 2008, the decision was made to begin encrypting laptops. In 2009, the process was halted due to financial constraints even though none of thousands of laptops had been encrypted. In 2010, the director of information security proposed restarting the encryption program following theft of a laptop and loss of records. However, no encryption had begun by August 2011. Encryption did begin slowly in May 2012. In June 2013, the compliance officer identified failure to encrypt ePHI as a high risk area. By November 2013, 4,400 computers remained unencrypted. As of January 2014, there still were 2,600 unencrypted computers.

The Judge Rejects Technical Arguments

Technical arguments presented by the center failed to sway the judge. It was a "red herring" for the center to argue that the regulations do not mandate encryption but, rather, allow flexibility in establishing security. The judge acknowledged encryption is not required, but he found that the center did not attempt to address security through an alternative mechanism. Once the center selected encryption, the judge said "it was obligated to make it work."

The judge similarly rejected an interpretation that "disclosure" required proof that the information was actually received by someone who lacked authorization. The judge ruled that HHS intended, and had the authority, to protect ePHI rather than "simply redress the consequences of unlawful disclosure."

The judge portrayed the center's argument as "fanciful" that the regulations did not apply to research information.

The judge found the center missed the point in arguing that the regulations should penalize the thief rather than the victim of the theft. The judge focused on the point that the case was about "failure to protect ePHI." (Emphasis in opinion.)

The judge approved two different types of penalties. The judge considered a penalty of US$2,000 per day to be justified for failure to protect ePHI under § 164.312(a). "The daily violations are the ongoing failure by Petitioner to protect patient ePHI from unauthorized disclosure, violations that persisted day after day for years." The imposed amount was "a small fraction of the maximum allowable daily amount of US$50,000" available under the regulations.

The judge approved an additional penalty for disclosure of ePHI in violation of § 164.502(a). The judge counted a violation of release separately "for each affected individual" rather than just three incidents of release, as argued by the center. The judge found it "makes no sense" to treat the release of data of many individuals as if the data pertained to only one person. When the number of releases was counted separately for each individual, this penalty easily reached the statutory maximum of US$1.5 million per year for identical violations.

The Message is Clear

The judge's decision teaches that implementing is less expensive and more efficient than repairing. HHS announced the judge's decision upholding a total penalty of US$4,348,000 with emphasis. The press release proclaimed "OCR is serious about protecting health information privacy and will pursue litigation, if necessary, to hold entities responsible for HIPAA violations." Entities covered by the regulations should take heed – and take action.

For more information about managing privacy and cybersecurity risks, including complying with HIPAA privacy and security requirements, please contact one of the lawyers listed in this article.

Stay current on trending issues and other developments impacting your business by subscribing to one or more of our industry-focused blogs including *Triage Health Law*, *Security & Privacy Bytes* and *The Anticorruption Blog*.

Contacts

Elliot R. Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

Tara Swaminatha
Partner, Washington DC
T +1 202 457 6031
E tara.swaminatha@squirepb.com

Thomas E. Zeno
Of Counsel, Cincinnati, Ohio
T +1 513 361 1202
E thomas.zeno@squirepb.com