King & Spalding
Client Alert

JULY 5, 2018

For more information, contact:

Marcia Augsburger
+1 916 321 4803
maugsburger@kslaw.com

King & Spalding

Sacramento
621 Capitol Mall
Suite 1500
Sacramento, CA 95814
Tel: +1 916 321 4800

Judge Grants Summary Judgment in Favor of OCR for HIPAA Violations Ordering a Texas Cancer Center to Pay $4.3 million in Penalties

On June 18, 2018, the U.S. Department of Health and Human Services (HHS) and its Office for Civil Rights (OCR) announced an Administrative Law Judge's (ALJ) ruling that OCR properly imposed penalties against The University of Texas MD Anderson Cancer Center (MD Anderson) for failing to encrypt laptops and USB thumb drives, in violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. One reason this decision is significant is that it may resolve an unsettled question: Is the use of encryption mandatory in the Security Rule? HHS's short answer has been "No," but based on the ALJ opinion, its long answer equates to "Yes" – at least when covered entities and business associates decide that encryption is necessary.

By way of background, whether encryption is required has long been unclear. For example, on the HHS website in response to the frequently asked question "Is the use of encryption mandatory in the Security Rule?," HHS first states "No," but then qualifies this answer: "The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI." https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html. The regulation adds to the confusion, stating in pertinent part at 45 C.F.R. § 164.312(a)(2):

A covered entity or business associate must, in accordance with § 164.306:

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or

software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) ***Implementation specifications: …***

(iv) ***Encryption and decryption (Addressable).*** Implement a mechanism to encrypt and decrypt electronic protected health information. (Emphasis and italics in original)

Subsection (2)(iv) seems to mandate encryption. Indeed, it does not contain the more flexible language that subsection (e)(2)(ii) includes regarding transmission of PHI: ***"Encryption (Addressable).*** Implement a mechanism to encrypt electronic protected health information **whenever deemed appropriate**." (Emphasis added). However, encryption is "addressable" under both subsections, and therefore not mandatory unless a risk assessment indicates it is reasonable and appropriate.

Adding to the confusion, Commentators and OCR itself have said that because encryption is now easily and inexpensively implemented, it must be considered reasonable and appropriate and therefore required and not simply a safe-harbor.

This was not, however, an argument OCR made in support of its imposition of penalties against MD Anderson. In fact, OCR noted, and the ALJ confirmed, that the regulations governing ePHI do not specifically require encryption. The ALJ added that covered entities have "considerable flexibility" in deciding how to protect ePHI.

Nonetheless, the ALJ ruled that OCR properly imposed penalties against MD Anderson for failing to encrypt data on all laptops and other devices. The penalties resulted from an investigation based on three incidents: On April 30, 2012, someone stole a "telework" laptop computer from an MD Anderson clinician's home; on July 13, 2012, a trainee lost, on an employee shuttle bus, a USB thumb drive that her supervisor authorized her to take home; and on or after November 27, 2013, a-visiting researcher also lost an USB thumb drive containing ePHI. The laptop contained PHI relating to almost 30,000 individuals and was neither encrypted nor password protected. The trainee's thumb drive was not encrypted and it contained ePHI relating to more than 2200 individuals. The researcher's unencrypted thumb drive contained information relating to about 3600 patients. However, these incidents were not in issue – or at least the penalties did not appear to be based on any determination that the incidents posed an appreciable risk of compromise constituting a breach.

OCR's imposition of penalties and the ALJ's decision turned on the evidence that MD Anderson recognized the need to encrypt data as early as 2006, determined that all devices should be encrypted, but then failed to promptly encrypt all of them. The ALJ opinion recites that MD Anderson consistently stated that confidential data must be protected against loss or theft; repeatedly announced a policy that both required encryption of confidential data and prohibited unsecured storage of such data; announced in 2008 that it intended to implement the first phase of a media security project that would test and implement encryption of institutional computers, but then delayed encryption and, according to the ALJ, "proceeded with encryption at a snail's pace," putting the process on hold in 2009 due to financial constraints. The opinion further recites that in 2010, citing the theft of a laptop and other incidents, MD Anderson's director of information security proposed restarting efforts to encrypt laptops, but nothing was done until August 2011 and that as of November 2013, more than ten percent of MD Anderson's computers remained unencrypted. However, these facts were largely unrelated to the penalties, which inexplicably ran from March 24, 2011 through January 25, 2013.

While OCR and the ALJ may have considered MD Anderson's financial and other reasons for delaying encryption as evidence that encryption of all devices was not then reasonable and appropriate, the ALJ did not say so. Moreover, no explanation is provided as to what, if anything, changed on March 24, 2011, and the decision appears to be based largely on the 2006 through 2010 occurrences described above. The ruling is based on the ALJ's opinion that once MD Anderson identified encryption as necessary and appropriate to reduce risk and implemented policies to ensure mobile

devices were encrypted, encryption became a “self-imposed” duty subject to enforcement and penalties for non-compliance – even if circumstances changed over time rendering encryption unreasonable.

> These facts establish that Petitioner, 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.. . . [D]espite this awareness and its own policies, Petitioner made only half-hearted and incomplete efforts at encryption over the ensuing years. As a consequence, the theft of a laptop computer that was not encrypted and the loss of two unencrypted USB thumb drives resulted in the unlawful disclosure of ePHI relating to tens of thousands of Respondent's patients.

However, again, the penalties did not run from the establishment of policies. Moreover, the ALJ suggested encryption was not the only choice, stating: “However, the bottom line is that whatever mechanisms an entity adopts must be effective.” Indeed, the ALJ acknowledged that “[n]othing in th[e] regulations directs the use of specific devices or specific mechanisms by a covered entity.”

MD Anderson contended that it was not required by regulation to encrypt its devices because 45 C.F.R. § 164.312(a)(2)(iv) only required that it "implement a mechanism to encrypt and decrypt electronic protected health information." (Emphasis added.) The cancer center argued it met this requirement by adopting and implementing a “mechanism" that included password protection of all computers that accessed potentially confidential information; an encryption requirement for confidential or protected data stored on portable computing devices; and annual employee training event that provided its employees with training about password necessity and integrity, among other relevant topics.

OCR relied on 45 C.F.R. § 164.312(a)(1), which states: “Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights ….” OCR asserted that MD Anderson violated the regulatory requirements because it failed to ensure that encryption of all laptop computers and USB drives. The ALJ agreed with OCR that the regulations require covered entities to “assure that all systems containing ePHI be inaccessible to unauthorized users.” Citing 45 C.F.R. § 164.306(a); 45 C.F.R. § 164.312(a)(1) (italics added). While these statements fall short of saying encryption is required, they express that this was OCR’s and the ALJ’s position. This is especially apparent from the placement of the ALJ’s findings in discussions about encryption, including for example: “[MD Anderson] failed to comply with regulatory requirements because it failed to adopt an effective mechanism to protect its ePHI [and going on to discuss encryption].”

Thus, the ALJ’s focus on MD Anderson’s acknowledgements between 2006 and 2010 that it should encrypt does not resolve the regulatory ambiguities. Further, the ALJ’s internally inconsistent analysis arguably creates more confusion in that on the one hand the ALJ acknowledged that encryption was not necessarily required while on the other, the ALJ penalized for failing to encrypt. Holding that the duty was “self-imposed” does not provide clarification in the context either. If a duty is “self-imposed,” an entity may conclude at various times that it is unreasonable to encrypt or to continue encrypting, thus relieving it of its “self-imposed” duty. In fact, MD Anderson was not penalized for failing to encrypt as set forth in its policies. While the opinion does not explain why the penalties ran from March 24, 2011 the opinion suggests that OCR chose March 24, 2011 as the first day of the violations to be “reasonable.” And certain statements by the ALJ suggest a conclusion that there were time before March 24, 2011 when MD Anderson was “compliant,” which may mean that during that period MD Anderson reasonably concluded encryption was not reasonable and appropriate under the circumstances.

For these reasons, the ALJ decision may have no precedential value in terms of guiding future encryption behaviors. At most, but nonetheless significantly, the decision certainly indicates that OCR may take the position that encryption is required if it is reasonable and appropriate under the circumstances or if an entity decides at any time that all devices should be encrypted and they are not at the time a potential breach occurs. This confirms what we knew before.

To summarize, the ALJ decision instructs that devices containing or accessing ePHI should be encrypted promptly after the entity determines that encryption is a reasonable and appropriate safeguard. It further informs that password protection will not be sufficient if the entity has decided encryption is reasonable and appropriate. The decision does not address situations where entities do not decide to encrypt or whether encryption is reasonable and appropriate in all cases. However, OCR's argument indicates it will likely rely on 45 C.F.R. § 164.312(a)(1) to require encryption where a covered entity or business associate fails to implement available safeguards to limit access only to those who are granted access rights.

We recommend that covered entities and business associates first fully and credibly analyze whether encryption of computers, thumb drives and similar devices, including cell phones that access PHI, is reasonable and appropriate, giving at least some consideration to OCR's position that encryption is required in at least some cases. If the entity decides encryption is reasonable and appropriate, staff should make sure that what they propose for implementation is achievable, and then ensure that their stated goals are achieved. If encryption is not reasonable or circumstances make it unreasonable, the reasons for such conclusions should be carefully and accurately documented. If encryption will occur over time or a decision is made not to encrypt, covered entities and business associates should also do everything possible to make sure that all systems containing ePHI are inaccessible to unauthorized users.

The ALJ's full opinion is available here: https://www.hhs.gov/sites/default/files/alj-cr5111.pdf