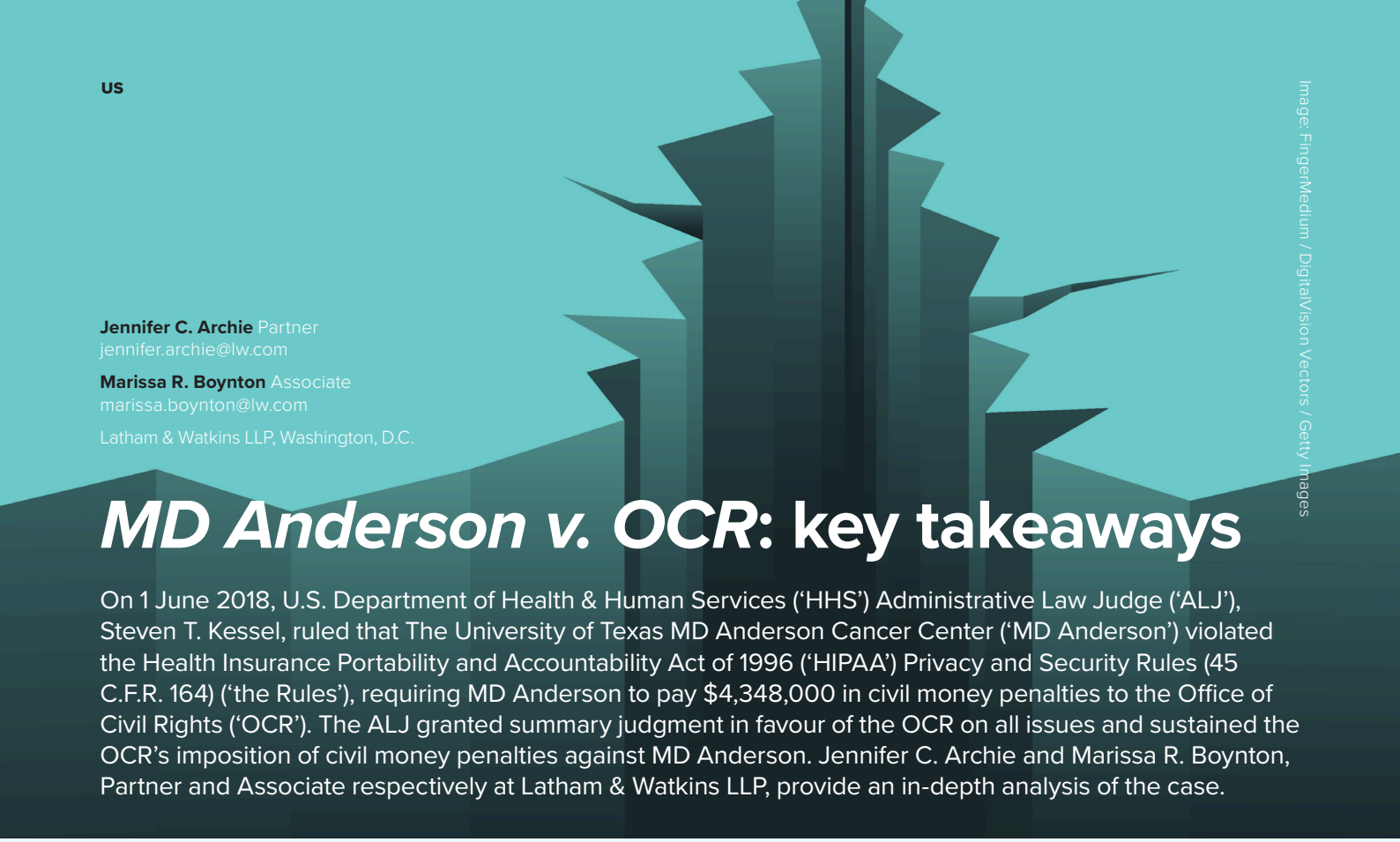

Image: FingerMedium / DigitalVision Vectors / Getty Images

Jennifer C. Archie Partner
jennifer.archie@lw.com

Marissa R. Boynton Associate
marissa.boynton@lw.com

Latham & Watkins LLP, Washington, D.C.

MD Anderson v. OCR: key takeaways

On 1 June 2018, U.S. Department of Health & Human Services ('HHS') Administrative Law Judge ('ALJ'), Steven T. Kessel, ruled that The University of Texas MD Anderson Cancer Center ('MD Anderson') violated the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') Privacy and Security Rules (45 C.F.R. 164) ('the Rules'), requiring MD Anderson to pay $4,348,000 in civil money penalties to the Office of Civil Rights ('OCR'). The ALJ granted summary judgment in favour of the OCR on all issues and sustained the OCR's imposition of civil money penalties against MD Anderson. Jennifer C. Archie and Marissa R. Boynton, Partner and Associate respectively at Latham & Watkins LLP, provide an in-depth analysis of the case.

Introduction

At the most basic level, *MD Anderson v. OCR* underscores the OCR's hardline approach to data breaches arising from loss or theft of unencrypted devices. As noted in Table I, fines and demands for corrective action are the rule, not the exception, following any significant data breach involving unencrypted devices. In its decision, the ALJ was sharply critical of MD Anderson's attempt to excuse the lack of encryption, stating:

"What is most striking about this case is that Respondent knew for more than five years that its patients' [electronic protected health information ('ePHI')] was vulnerable to loss and theft and yet, it consistently failed to implement the very measures that it had identified as being necessary to protect that information. Respondent's dilatory conduct is shocking given the high risk to its patients resulting from unauthorized disclosure of ePHI, a risk that MD Anderson not only recognized but that it restated many times."

This proceeding is very notable procedurally and one that covered entities and business associates under HIPAA will want to follow closely if MD Anderson appeals. MD Anderson likely chose to contest the proposed action in order to set up an eventual appeal to the federal district court on key questions concerning:

- the 'addressable' security control of encryption set forth in the Rules;
- whether the theft or loss of a device, without evidence that a third party actually accessed or acquired the data stored on the device constitutes an unlawful 'disclosure' under the rule; and
- the reasonableness of the formulas the OCR applies to calculate civil money penalties.

The case highlights OCR's unwavering approach to a covered entity's failure to encrypt ePHI on devices, notwithstanding the technical legal challenges under the wording of HIPAA or the Rules, and potentially sets up a legal battle in federal court.

Background

MD Anderson is both an academic institution and a cancer treatment and research centre located at the Texas Medical Center in Houston, Texas. MD Anderson is a covered entity under HIPAA and creates, maintains, receives and transmits ePHI related to its patients who receive health care services from MD Anderson.

MD Anderson submitted breach notification reports to the OCR in 2012 and 2013 in connection with three separate breach incidents affecting a total of 34,883 individuals. The first breach occurred on 30 April 2012 when an MD Anderson employee reported the theft of his laptop computer from his personal residence. The laptop was not encrypted or password-protected and contained the ePHI for 29,021 individuals. The second breach occurred on 13 July 2012 and involved the loss of a USB thumb drive by an MD Anderson intern containing the ePHI for 2,264 individuals. The third breach occurred on 2 December 2013, involving the loss of an unencrypted USB thumb drive containing the ePHI for 3,598 individuals.

Between October 2015 and August 2016, MD Anderson and the OCR attempted to reach a resolution on the matter, but this proved unsuccessful. On 24 March 2017, the OCR issued a notice of proposed determination suggesting that MD Anderson pay over $4.3 million in civil money penalties. MD Anderson subsequently requested an administrative hearing.

ALJ opinion

The OCR alleged that MD Anderson had failed to comply with the HIPAA regulatory requirements in two ways:

- by failing to protect its ePHI by not performing its self-imposed duty to encrypt electronic devices and data storage equipment (§164.312 of the Rules); and
- by allowing ePHI to be impermissibly disclosed (§164.502(a) of the Rules).

The ALJ agreed with both assertions, rejecting MD Anderson's arguments. The ALJ relied on MD Anderson's well

Ultimately, *MD Anderson v. OCR* amounts to MD Anderson's failure to encrypt portable devices after identifying the risk of loss or theft and deciding that encryption was the appropriate method for mitigating the risk.

documented, long-standing security assessment that encryption of portable devices storing ePHI was an important and specifically selected means to mitigate risk of unauthorised disclosure. In addition, he highlighted that:

- MD Anderson's 2006 version of its Information Resources Security Operations Manual required that data stored on transportable media and laptops must be encrypted;
- in 2008, MD Anderson announced that it intended to implement the first phase of a media security project which included implementing encryption of institutional laptop and desktop computers;
- in 2009, MD Anderson put laptop encryption efforts on hold due to financial constraints. As of then, it had not encrypted any of its laptops. In 2010, MD Anderson's director of information security proposed restarting efforts to encrypt laptops in light of the theft of a laptop and other instances of lost records; and
- as of November 2013, following the three breaches reported to the OCR, more than 4,400 MD Anderson computers were not encrypted, and as of January 2014 more than 2,600 MD Anderson computers were not encrypted.

MD Anderson argued that it was not required to encrypt its devices as Section 164.312(a)(2)(iv) of the Rules only requires covered entities to "implement a mechanism to encrypt and decrypt electronic protected health information." Under the Rules, encryption is an 'addressable' security standard, which means that MD Anderson could theoretically have attempted to document and justify an alternative security mechanism that was equivalent to encryption, including on grounds of expense or burden. Here, however, it seems that for many years MD Anderson had selected encryption as its preferred mechanism and had not documented an effective implementation of alternative means. Covered entities put themselves at risk when they decide to use addressable controls for encryption. Furthermore, MD Anderson was unsuccessful in its argument that it had implemented a legally adequate "mechanism" by:

- requiring confidential data and ePHI stored on portable computing devices be encrypted and backed up;
- employing password protection; and
- providing annual employee training regarding securing and protecting ePHI.

While the ALJ agreed that risks can be mitigated through mechanisms other than encryption, it found that a covered entity must adopt a mechanism that is effective at protecting its ePHI, which MD Anderson had failed to do in his opinion. Whenever the root cause of an unauthorised disclosure of ePHI is the loss of an unencrypted device, the covered entity will have a very hard time prevailing on the argument that these alternative methods were equivalent, reasonable and appropriate.

MD Anderson further argued that it did not violate §164.502(a) of the Rules because:

- the loss of ePHI from the stolen laptop and lost thumb drives was not a 'disclosure' as defined by the Rules absent factual evidence that an unauthorised person viewed the data (as opposed to being in mere possession of the devices);
- the ePHI contained in the stolen and lost devices was research information that is outside the scope of HIPAA and the Rules; and
- unsanctioned activities by its employees and by the person who stole the laptop cannot be imputed to MD Anderson.

The ALJ rejected all three arguments. While the absence of evidence that bad actors had access to the data can sometimes support an argument that the data subjects were not harmed by the loss of security, the ALJ disagreed that such proof was needed in order to conclude the ePHI was 'disclosed.' The ALJ also dismissed MD Anderson's argument that the lost or stolen ePHI was research information and therefore outside the scope of HIPAA and the Rules. MD Anderson tried to rely on language in the Rules' preamble regarding research, however, the ALJ determined that such language was meant to apply to research conducted by non-covered entities. Lastly, the ALJ rejected MD Anderson's argument that it could not be held liable since its employees who lost the thumb drives were not acting within the scope of their authorised duties, and the thief who stole the laptop was not an agent or employee of MD Anderson. The ALJ clarified that while MD Anderson's employees contravened the company's policies concerning protection of ePHI, this does not mean that their actions were outside the scope of their official duties. With regard to the stolen laptop, the ALJ made clear that the gravamen of the case is not the theft itself but the fact that MD Anderson failed to protect ePHI from disclosure.

MD Anderson also made several arguments against the penalty requests submitted by the OCR, all of which were rejected by the ALJ. The OCR determined that MD Anderson's violations qualified them for the second tier of penalty ranges, namely violations that "are due to reasonable cause and not due to willful neglect." MD Anderson attempted to argue that, to the extent that any violation occurred, it should fall within the first tier of non-compliance which is for violations that "the covered entity did not know about or would not have known about by exercising reasonable due diligence." MD Anderson's argument turned on the fact that it could not have known that a thief would steal a laptop or that its employees would choose to use unencrypted USB drives for storage of confidential information and then lose those devices. While the ALJ acknowledged that MD Anderson could not foresee those acts, it dismissed the argument as irrelevant.

The issue was whether MD Anderson was aware of the risk posed by storing unencrypted ePHI on mobile devices. The ALJ concluded definitively that MD Anderson was aware of this risk evidenced by, among other things, the fact that in 2008 it had ordered that all mobile devices be encrypted. The ALJ rejected MD Anderson's attempts to

Figure 1: Fines issued to healthcare organisations following a data breach

Name of entity	# of individuals affected	Settlement amount/penalty	Resolution year
Providence Health & Services	386,000	$100,000	2008
Blue Cross Blue Shield of Tennessee	1,000,000	$1,500,000	2012
Alaska Department of Health & Social Services	501	$1,700,000	2012
Massachusetts Eye & Ear Infirmary and Massachusetts Eye & Ear Associates, Inc.	3,594	$1,500,000	2012
Hospice of North Idaho	441	$50,000	2013
Adult & Pediatric Dermatology, P.C.	2,200	$150,000	2013
Concentra Health Services	870	$1,725,220	2014
QCA Health Plan, Inc., of Arkansas	148	$250,000	2014
St. Elizabeth's Medical Center	595	$218,400	2015
Cancer Care Group, P.C.	55,000	$750,000	2015
Lahey Hospital and Medical Center	599	$850,000	2015
North Memorial Health Care	9,497	$1,550,000	2016
Feinstein Institute for Medical Research	13,000	$3,900,000	2016
Catholic Health Care Services of the Archdiocese of Philadelphia	412	$650,000	2016
Advocate Health Care Network	4,029,530	$5,550,000	2016
MAPFRE Life Insurance Company of Puerto Rico	2,209	$2,204,182	2017
Children's Medical Center of Dallas	6,262	$3,200,000	2017
CardioNet	3,610	$2,500,000	2017
The University of Texas MD Anderson Cancer Center	34,883	$4,348,000	2018

continued

turn the penalty question into an issue of whether the employees had abided by its policies. Whether or not they had abided by the policies does not change the fact that MD Anderson had failed to address the risk that it had identified, the potential for data loss due to the storage of ePHI on unencrypted devices.

The OCR requested that the ALJ impose two penalties falling within the ranges permitted by the second tier: penalties of $2,000 per day for the period of 24 March 2011 to 25 January 2013, to remedy MD Anderson's failure to encrypt ePHI; and penalties of $1,500,000 per year for the years 2012 and 2013, to remedy the loss of ePHI pertaining to approximately 31,000 and 3,500 individuals respectively.

The ALJ acknowledged that a penalty of $2,000 per day is reasonable given MD Anderson's level of culpability, and that it is only a small fraction of the $50,000 per day penalty that is allowed for second tier penalties. Again, the ALJ noted that MD Anderson had failed to implement encryption on mobile devices for years after identifying the risk, and the unauthorised disclosure affected over 33,000 individuals. The ALJ rejected MD Anderson's argument that, at most, it had committed three violations of regulatory requirements. In addition, it clarified that the violations did not result from the specific events resulting in the data breaches, but instead, from MD Anderson's failure to protect the ePHI for several years.

Furthermore, the ALJ held that a penalty of $1,500,000 per year for the years 2012 and 2013 was appropriate. The ALJ considered the loss of ePHI on a per capita basis to reflect the gravity of the loss. It also concluded that any mitigating factors cited by MD Anderson were taken into consideration, evidenced by the fact that $2,000 per day is only 1/25th of the maximum allowable penalty, and the annual penalties of $1,500,000 come out to less than $90 for each violation.

Takeaways for future cases

Ultimately, *MD Anderson v. OCR* amounts to MD Anderson's failure to encrypt portable devices after identifying the risk of loss or theft and deciding that encryption was the appropriate method for mitigating the risk. The ALJ repeated this point throughout its decision, sending a clear message to all covered entities: do not delay implementing measures to protect your ePHI once an area has been identified as high risk, and particularly, once you have decided how to address the risk.

Also, speaking at the American Health Lawyers Association Annual Meeting on 26 June 2018, Serena Mosely-Day, Acting Senior Advisor for HIPAA Compliance and Enforcement at the OCR, stated that *MD Anderson v. OCR* stands for the failure to manage an identified risk to prevent future impermissible disclosures.