Morgan Lewis

FAST BREAK: HIPAA ENFORCEMENT CASE ANALYSIS – *MD ANDERSON CANCER CENTER V OCR*

Scott McBride, Krista Barnes
and Jake Harper
March 31, 2021

Morgan Lewis

TODAY'S PRESENTERS

Scott McBride
Partner
Morgan Lewis

Krista Barnes
Deputy Chief Compliance Officer
The University of Texas MD Anderson Cancer Center

HIPAA Enforcement Case Analysis – *MD Anderson Cancer Center v OCR*

Topics to be discussed today include

- **Important case background information**
- **Legal argument presented by the parties**
- **Discussion of the decision**
- **Impact of the decision on enforcement activities**

Case Overview

OCR imposed a Civil Money Penalty (CMP) in the amount of $1,500,000 for alleged "disclosure" violations in 2012 related to a stolen laptop and a lost USB drive.

It is undisputed that there was no harm to any individuals relating to these alleged disclosure violations, nor is there any evidence that information on either device was accessed by another person.

For these alleged violations, the CMP was calculated at $1,000 per person.

The CMP of $1,500,000 for this violation is the maximum amount that the OCR could impose, making the punishment the same as in a case in which ePHI was intentionally taken to cause harm to the patients and where harm was actually incurred.

Case Overview

OCR imposed a CMP in the amount of $1,500,000 for alleged "disclosure" violations in December 2013 related to a lost USB drive.

It is undisputed that there was no harm to any individuals relating to this alleged disclosure violation, nor is there any evidence that information on the device was accessed by another person.

The proposed CMP involves an employee who was trained on properly securing ePHI and who was furnished an encrypted USB drive, although she chose not to use it.

The CMP was calculated at $1,000 per person.

The CMP of $1,500,000 imposed for this violation is the maximum amount that the OCR could impose.

Case Overview

OCR also imposed a CMP in the amount of $1,348,000 for alleged "encryption" violations for the period of time from March 24, 2011, through January 25, 2013.

This alleged violation involves an addressable standard.

For this alleged violation, the CMP was calculated at $2,000 a day and at a culpability level of "reasonable cause."

Enforcement Landscape

Feb. 2011
Mass General: $1 million fine, CAP.
192 patients' information contained in documents left on train, including HIV information.

March 2012
BCBS TN: $1.5 million fine, CAP.
Theft of 57 unencrypted hard drives with 1 million individuals' PHI.

March 2016
Feinstein Institute: $3.9 million fine, CAP.
Unencrypted laptop stolen.

July 2016
OHSU: $2.7 million fine, CAP.
Two unencrypted laptops; one unencrypted USB drive; PHI stored in unauthorized cloud storage location.

August 2016
Advocate Health Care: $5.55 million fine, CAP.
Four unencrypted desktops, one unencrypted laptop stolen.

Enforcement Landscape

Feb. 2017
Dallas Children's: $3.2 million
Loss of an unencrypted, non-password protected Blackberry.
Chose to pay fine – no settlement.

March 2017
MDACC NPD: $4.3 million fine proposed.
MDACC appealed.

May 2017
Memorial Hermann: $2.4 million fine, CAP.
Disclosed PHI in a press release without auth.

Dec. 2017
21st Century Oncology: $2.3 million fine, CAP.
Database hacked, 2.2 million records on dark web.

Oct. 2018
Anthem: $16 million fine, CAP.
Cyber-attackers gained access to IT systems. ePHI of 79 million individuals stolen.

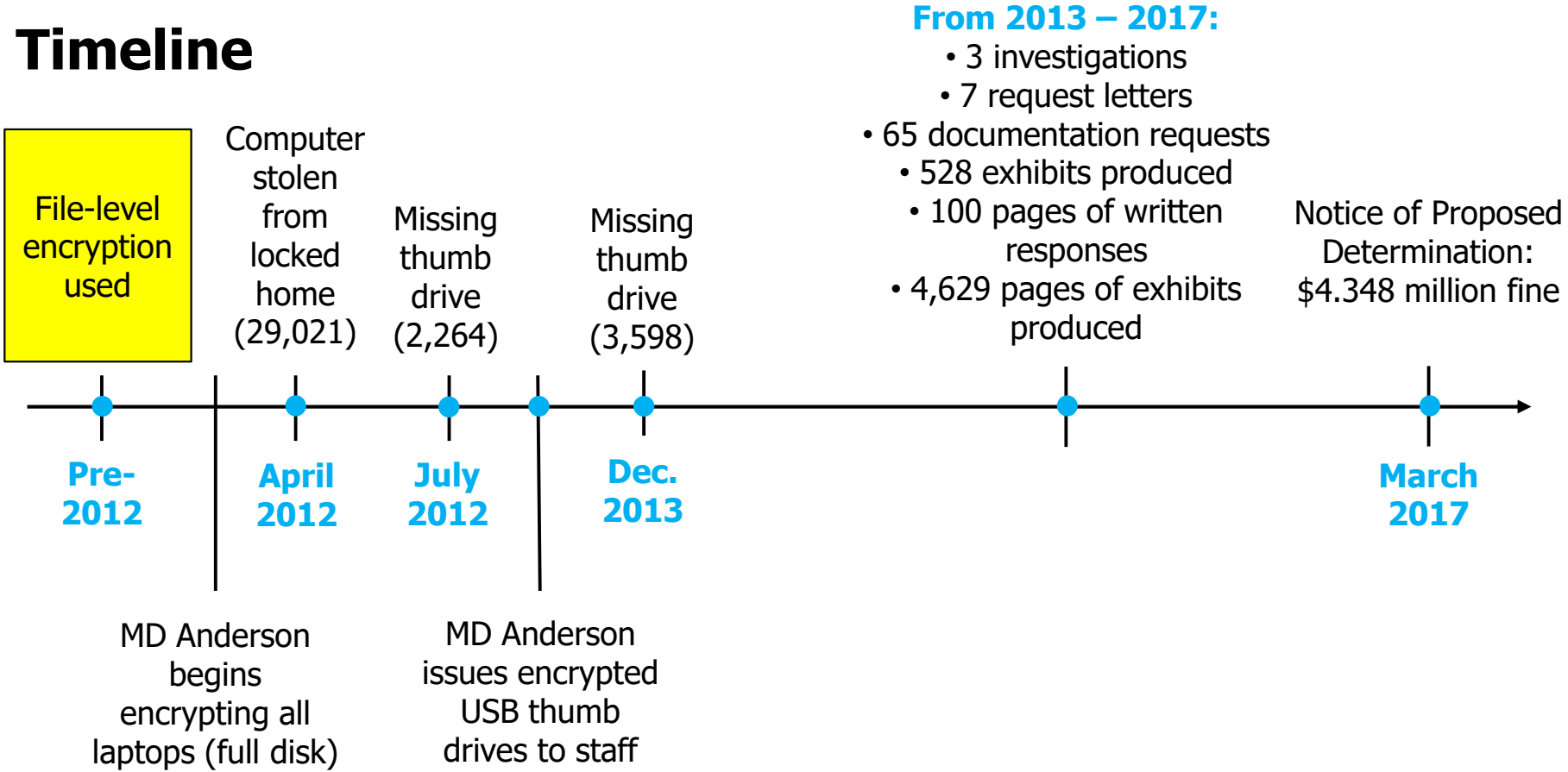
And yet…

In 2014, Cedars-Sinai Health System reported that an employee's unencrypted laptop computer was stolen during a residential burglary. The OCR reports that the laptop contained the electronic protected health information of approximately 33,136 individuals. Cedars-Sinai provided breach notification to HHS, affected individuals, and the media, and posted notice of the incident on its website. Cedars-Sinai reported no identity theft or other misuse of the potentially affected information resulting from this incident. Following the OCR's investigation, Cedars-Sinai updated its policies and procedures related to the storage, transmission and encryption of ePHI, as well as the enforcement of its employees' adherence to these policies and procedures. Based on foregoing, the OCR closed its case and assessed no penalty.

And yet…

In 2015, North East Medical Services reported that an unencrypted laptop computer used to store electronic protected health information was stolen from a workforce member's car. The laptop reportedly stored ePHI associated with 69,246 individuals. The ePHI included patients' names, dates of birth, genders, contact information, payers/insurers, diagnoses, medications, treatment information, test results, appointment information, and, in some cases, social security numbers. North East Medical Services provided breach notification to HHS, affected individuals, and the media. The OCR reports that **"as an alternative to encryption, NEMS had implemented a policy that no ePHI was to be stored on unencrypted laptops, workstations, other personal devices, or external media. Unfortunately, without knowledge of NEMS administration, a workforce member violated this policy."** In response to the breach, North East Medical Services implemented encryption technology, updated its policies, strengthened passwords requirements, and performed a risk assessment. Based on foregoing, the OCR closed its case and assessed no penalty.

Timeline


From 2013 – 2017:
• 3 investigations
• 7 request letters
• 65 documentation requests
• 528 exhibits produced
• 100 pages of written responses
• 4,629 pages of exhibits produced
File-level encryption used
Computer stolen from locked home (29,021)
Missing thumb drive (2,264)
Missing thumb drive (3,598)
Notice of Proposed Determination: $4.348 million fine
Pre-2012
April 2012
July 2012
Dec. 2013
March 2017
MD Anderson begins encrypting all laptops (full disk)
MD Anderson issues encrypted USB thumb drives to staff

Information Security Controls in 2012

Administrative controls:	Policies prohibited storing PHI on devices
Physical security:	Badge access, docking stations with locks
Technical security (4 layers):	Infrastructure/network layer, application layer, file layer, and device layer • **Network layer:** Firewalls, virus scanning, patch management • **Application layer:** Role-based access to systems containing PHI, login/password protection, automatic logoffs • **File layer:** Email and file level encryption • **Device layer:** Logins and passwords required, began full-disk encryption project in May 2010 ➢ Issued RFPs, hired consultants to evaluate compatible technology ➢ Planned and tested technology ➢ Full-disk encryption rollout begins August 2011, complete August 2012 ➢ 5,000 encrypted IronKey drives purchased July 31, 2012

Notice of Proposed Determination

In March of 2017, the OCR issued a Notice of Proposed Determination, in which it proposed a $4.3 million fine for:

- Failure to implement encryption in violation of 45 CFR 164.312(a)(2)(iv)
  – $1.348 million penalty
  (*i.e.,* $2,000 per day from 3/24/2011 to 1/25/2013)

- Disclosure of 34K individuals' PHI in violation of 45 CFR 164.502(a)
  – $3.0 million ($1.5 million cap for two years)
  *(i.e., $*1,000 per individual whose PHI was involved)

- The OCR acknowledged that there was no harm to individuals.

Encryption

Whether MD Anderson violated the Access Control Standard at 45 CFR § 164.312(a)(1) by failing to implement a mechanism for encryption pursuant to 45 CFR § 164.312(a)(2)(iv).

MD Anderson:	The regulation says encryption is "addressable" (as opposed to "required"). The preamble talks about flexibility. MDACC used *file level* encryption until it moved to *device level* encryption.
ALJ/DAB:	"[MDACC] failed to perform its *self-imposed* duty to encrypt electronic devices…" "Having chosen that mechanism to meet the encryption requirement, MDA was required to fully implement it, not some other mechanism."

Encryption

Whether MD Anderson violated the Access Control Standard at 45 CFR § 164.312(a)(1) by failing to implement a mechanism for encryption pursuant to 45 CFR § 164.312(a)(2)(iv).

5th Circuit:	"Petitioner plainly implemented "a mechanism" to encrypt ePHI." The Court noted that "the Government argues that the stolen laptop and the two lost USB drives were not encrypted at all. . . . But that does not mean M.D. Anderson failed to implement "a mechanism" to encrypt ePHI." "The regulation requires only "a mechanism" for encryption. It does not require a covered entity to warrant that its mechanism provides bulletproof protection of all systems containing ePHI." The Court concluded that "M.D. Anderson satisfied HHS's regulatory requirement, even if the Government now wishes it had written a different one."

Disclosure

Whether any of the three incidents at issue constitute a "disclosure" of ePHI for the purposes of the Uses and Disclosures of Protected Information Standard at 45 CFR § 64.502(a).

The Regulation:	"Disclosure" = "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 CFR 160.103.
MD Anderson:	This is a specific definition that the OCR has not met. There's no evidence that anyone outside of MD Anderson ever actually *saw* the PHI on those misplaced and stolen devices.
DAB:	"Nothing in this definition or in the regulatory definition of disclosure requires that lost ePHI be read, accessed by or provided to anyone outside of the covered entity."

Disclosure

Whether any of the three incidents at issue constitute a "disclosure" of ePHI for the purposes of the Uses and Disclosures of Protected Information Standard at 45 CFR § 64.502(a).

OCR:	"MD Anderson employees and/or contractors provided access to MD Anderson's ePHI when they **lost control** of devices containing ePHI and/or left such devices unattended. Since the devices containing ePHI were lost or stolen, and were never recovered, they are no longer in MD Anderson's possession and are unprotected from an unauthorized person, therefore, MD Anderson "provided access" to the ePHI." **"Loss of Control"** OMB Memorandum M-07-16

Disclosure

Whether any of the three incidents at issue constitute a "disclosure" of ePHI for the purposes of the Uses and Disclosures of Protected Information Standard at 45 CFR § 64.502(a).

5th Circuit:	HHS's "interpretation departs from the regulation HHS wrote in at least three ways. First, each verb HHS uses to define "disclosure"—release, transfer, provide, and divulge—suggests an affirmative act of disclosure, not a passive loss of information." "It defies reason to say an entity affirmatively acts to disclose information when someone steals it. That is not how HHS defined "disclosure" in the regulation." The Court then noted that "the Government nowhere explains how "information" can be released, transferred, provided, or divulged without someone to receive it and hence be informed by it. To the contrary, the regulation appears to define "disclosure" in accordance with its ordinary meaning, which requires information to be "made known" to someone."

Statutory Caps on CMPs

The Proposed CMP Violates the Statutory Caps.

MD Anderson:

The OCR is assessing CMPs in amounts that are beyond the statutory limits.

- The OCR incorrectly interpreted § 1320d-5 as authorizing an identical annual cap of $1,500,000 for violations *no matter the level of culpability*. The language of § 1320d-5 does not support the OCR's position.
- The disregard of the culpability-specific caps in § 1320d-5 has led to a proposed CMP against MD Anderson that is nearly *ten times* more than the maximum permitted under the statute.

ALJ/DAB:

The argument is beyond our authority to decide.

Statutory Caps on CMPs

The Proposed CMP Violates the Statutory Caps.

After filing the appeal but prior to oral arguments, OCR issued a Notice of Enforcement Discretion in response to MD Anderson's longstanding argument that the OCR was incorrectly applying statutory caps.

5th Circuit:	Even though HHS recognized its error in a notice of "enforcement discretion", this "does nothing to change the text of the regulations HHS promulgated through notice and comment. Nor does it cure the erroneous premises of the decisions by the ALJ and the Departmental Appeals Board." The Court went on to list the factors considered when assessing CMPS, such as physical harm, financial harm, reputation, and ability to obtain health care. The Court found that "It's undisputed that HHS can prove none of these."

Eighth Amendment

The proposed CMP is excessive in violation of the Eighth Amendment of the U.S. Constitution.

MD Anderson:	CMP is excessive in violation of the 8th Amendment of US Constitution. • "Excessive bail shall not be required, nor excessive fines imposed…" • Consider actual harm caused by the offense
ALJ:	I have no authority to address this argument. But . . . . "the annual penalties of $1,500,000 appear to be large but comes to less than $90 for each violation committed by [MDACC]."

Arbitrary and Capricious

The Proposed CMP Is Arbitrary and Capricious.

MD Anderson:	The enforcement by the OCR is arbitrary and capricious. There are many circumstances with more violations, yet lower or no fines.
DAB:	There is "'nothing in the regulations that suggests' that the ALJ 'evaluate penalties based on a comparative standard…'"

Arbitrary and Capricious

The Proposed CMP Is Arbitrary and Capricious.

5th Circuit:	"It is a bedrock principle of administrative law that an agency must treat 'like cases' alike." "In this case, M.D. Anderson proffered examples of other covered entities that violated the Government's understanding of the Encryption Rule and faced zero financial penalties. For example, a Cedars-Sinai employee lost an unencrypted laptop containing ePHI for more than 33,000 patients in a burglary. HHS investigated and imposed no penalty at all. The Government has offered no reasoned justification for imposing zero penalty on one covered entity and a multi-million-dollar penalty on another." The Court concluded that if it were otherwise, "an agency could give free passes to its friends and hammer its enemies—while also maintaining that its decisions are judicially unreviewable because each case is unique. Suffice it to say the APA prohibits that approach."

State Agency

Whether the OCR is authorized under 42 U.S.C § 1320d-5 to impose a CMP against MD Anderson, which is an agency of the State of Texas.

MD Anderson:	The statute doesn't allow the Secretary to impose a CMP against a state or state agency. It says "person" and a state agency is not a "person" under the statutory definition. • "Person means an individual, a trust or estate, a partnership, or a corporation." – 42 USC 1301(a)(3). • OCR revised the regulations to include states, but lacks statutory authority to do so.
ALJ/DAB:	We have no authority to address this argument.

State Agency

Whether the OCR is authorized under 42 U.S.C § 1320d-5 to impose a CMP against MD Anderson, which is an agency of the State of Texas.

This was the primary focus of oral arguments. The 5th Circuit requested additional briefing on the issue.

5th Circuit:	For the purpose of this opinion, we will assume MD Anderson is a "person" under the statute. The issue is not resolved and remains to be litigated another day. In our briefing, we requested that the Court issue substantive decisions to the healthcare industry.

Now What?

- While healthcare providers may take some comfort in the decision's conclusion that the regulations do not create strict liability or require a "bullet proof" mechanism of protection, they should continue to be vigilant in maintaining patient privacy and security.
  - Document the lack of evidence of any harm
  - Document the lack of evidence of any information being accessed by anyone outside the entity
  - Document the mechanisms in place to address encryption
- The decision will not lessen any of the focus and vigilance of healthcare providers to continue to protect patient information.

Join us next month!

Please join us for next month's webinar:

***Fast Break:* Returning to Work**

Featuring

Daniel Kadish and Jake Harper

- Tuesday, April 27, 2021 3:00 PM (EST)

Morgan Lewis

QUESTIONS?

Thanks and Be Well!

Krista Barnes

AVP & Deputy Chief Compliance Officer

The University of Texas MD Anderson Cancer Center

Krista is the AVP & Deputy Chief Compliance Officer at MD Anderson Cancer Center. Prior to her current role, she served as the Senior Legal Officer responsible for privacy and information security compliance at MD Anderson from 2012 – 2018. From 2004 - 2012, Krista was a health law associate in the Houston offices of Vinson & Elkins, Baker & Hostetler, and King & Spalding, focusing primarily on Medicare reimbursement litigation and compliance with state and federal health care laws. Krista attended Rice University and Duke University School of Law.

Thanks and Be Well!

Scott McBride
Partner
Houston
+1.713.890.5744
scott.mcbride@morganlewis.com
Click Here for full bio

Scott provides legal services to clients throughout the healthcare industry, with a focus on compliance and enforcement issues. Scott represents and advises hospitals, academic medical centers, physician groups, and other healthcare clients in overpayment disputes, False Claims Act (FCA) litigation, internal and external investigations, and regulatory enforcement proceedings. His work spans a variety of matters related to Medicare and Medicaid billing compliance, civil monetary penalties, Stark Law and the Anti-Kickback Statute, corporate oversight, and exclusions from federal and state healthcare programs.

Thanks and Be Well!

Jake Harper
Associate
Washington, DC
+1.202.739.5260
jacob.harper@morganlewis.com
Click Here for full bio

Jake advises stakeholders across the healthcare industry, including hospitals, health systems, large physician group practices, practice management companies, hospices, chain pharmacies, manufacturers, and private equity clients, on an array of healthcare regulatory, transactional, and litigation matters. His practice focuses on compliance, fraud and abuse, and reimbursement matters, self-disclosures to and negotiations with OIG and CMS, internal investigations, provider mergers and acquisitions, and appeals before the PRRB, OMHA, and the Medicare Appeals Council.