DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (214) 767-4056, (800) 368-1019
TDD - (214) 767 8940, FAX - (214) 767-0432
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Southwest Region
1301 Young Street, Suite 1169
Dallas, TX 75202

Via UPS #1ZR7937W0190283274

March 24, 2017

Mr. Scott McBride
Baker and Hostetler
811 Main Street, Suite 1100
Houston, Texas 77002-1717

RE: OCR Transaction Numbers 12-145395, 12-147543, and 14-175214

NOTICE OF PROPOSED DETERMINATION

Dear Mr. McBride:

Pursuant to the authority delegated by the Secretary of the United States Department of Health and Human Services (HHS) to the Office for Civil Rights (OCR), we are writing to inform you that OCR is proposing to impose a civil money penalty (CMP) of $4,348,000 against The University of Texas MD Anderson Cancer Center (MD Anderson).

This proposed action is being taken under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), § 262(a), Pub.L. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Section 13410, *codified at* 42 U.S.C. § 1320d-5, and under 45 C.F.R. Part 160, Subpart D.

I. The Statutory Basis for the Proposed CMP

The Secretary of HHS is authorized to impose CMPs (subject to the limitations set forth at 42 U.S.C. § 1320d-5(b)) against any covered entity or business associate, as described at 42 U.S.C. § 1320d-1(a), that violates a provision of Part C (Administrative Simplification) of Title XI of the Social Security Act. *See* HIPAA, § 262(a), as amended, 42 U.S.C. § 1320d-5(a). This includes violations of the regulations commonly known as the Privacy, Breach Notification, and Security Rules, promulgated at 45 C.FR Part 160 and Subparts A, C, D, and E of Part 164 (the "HIPAA Rules"), pursuant to Section 264(c) of HIPAA. The Secretary has delegated enforcement responsibility for

the HIPAA Rules to the Director of OCR. *See* 65 Fed. Reg. 82,381 (Dec. 28, 2000) and 74 Fed. Reg. 38630 (July 27, 2009). OCR is authorized under the HITECH Act, Section 13410, 42 U.S.C. § 1320d-5(a)(3), to impose CMPs for violations occurring on or after February 18, 2009, of:

- A minimum of $100 for each violation where the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.
- A minimum of $1,000 for each violation due to reasonable cause and not to willful neglect, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000. Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.
- A minimum of $10,000 for each violation due to willful neglect and corrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.
- A minimum of $50,000 for each violation due to willful neglect and uncorrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

II. Findings of Fact

1. MD Anderson is a "covered entity" within the definition set forth at 45 C.F.R. § 160.103, and, as such, is required to comply with the requirements of the Privacy, Security and Breach Notification Rules.
2. MD Anderson is headquartered in Houston, Texas. It operates six cancer treatment hospitals and two diagnostic imaging clinics in the Greater Houston area, including its Texas Medical Center location, the main hospital campus of MD Anderson.
3. MD Anderson creates, maintains, receives, and transmits protected health information (PHI) related to its patients who receive health care services from workforce members of MD Anderson.
4. MD Anderson submitted Breach Notification Reports ("Reports") to the Office for Civil Rights (OCR) in 2012 and 2013 in connection with

three separate breach incidents that occurred affecting a total of 34,883 individuals.

5. The first breach occurred on April 30, 2012, and involved the theft of an unencrypted laptop computer that contained the electronic protected health information (ePHI) for 29,021 individuals. The MD Anderson physician/faculty member, Dr. Randall Millikan, reported the theft of the laptop from his personal residence on May 1, 2012. Dr. Millikan purchased this laptop with funds provided by MD Anderson and used it as a telework computer. Dr. Millikan acknowledged that his stolen laptop was never encrypted or password-protected. Further, he stated that the laptop was not otherwise secured and that any family member could have accessed ePHI on his laptop.
6. The second breach occurred on July 13, 2012, and involved the loss of an unencrypted universal serial bus (USB) thumb drive that contained the ePHI for 2,264 individuals. An MD Anderson trainee, specifically, an MD Anderson summer intern in the Department of Stem Cell Transplantation and Cellular Therapy, reported that she misplaced a thumb drive to which she had uploaded MD Anderson's ePHI on July 13, 2012. The trainee used the drive to store Microsoft Excel files containing ePHI and believes that she misplaced the drive on her way home from work on July 12, 2012.
7. The third breach occurred on December 2, 2013, and also involved the loss of an unencrypted USB thumb drive. This thumb drive contained the ePHI for 3,598 individuals. On December 2, 2013, Dr. Marisa Gomes, a visiting researcher from Brazil, notified her Department Administrator (Infectious Disease Department) that she was unable to find a personally-owned USB thumb drive to which she had uploaded MD Anderson ePHI and that she had kept in a tray in her desk. She reported that she had last seen the thumb drive on the afternoon of November 27, 2013, when she left work for Thanksgiving break, and was unable to find it when she returned the morning of December 2, 2013.
8. 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 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.
9. At the time of the above-mentioned breach incidents, MD Anderson had written policies that included certain encryption requirements. Such requirements are contained in MD Anderson's "Information Resources Security Operation Manual" dated July 30, 2007, an "Information Resources Acceptable Use Agreement and User Acknowledgment" dated January 27, 2009, and employee newsletters as far back as 2010.

10. Despite the existence of encryption requirements for the security of ePHI, MD Anderson did not begin to implement an enterprise-wide solution to meet those encryption requirements described in the policies and newsletters until August 2011, when it launched its encryption project for all desktops and laptops. In spite of the fact that MD Anderson experienced three separate major breaches in 2012 and 2013, it still failed to achieve complete encryption of its inventory of electronic devices containing ePHI as of January 25, 2013. As of that date, MD Anderson reported to OCR that it had encrypted 98% of its total managed computer inventory (33,385 computers).[1]
11. Prior to the occurrence of the three breaches in 2012 and 2013 referenced above, MD Anderson had actual knowledge that ePHI should have been protected by encryption, but failed to implement the encryption required. MD Anderson's Information Security Program and Annual Reports (the "Reports") for calendar years 2010-2011 identified encryption of confidential data on mobile media as a key risk area that is "currently not mitigated." Likewise, a subsequent risk analysis also indicated problems concerning the security of ePHI. MD Anderson's Corporate Compliance Risk Analysis for fiscal year 2011 (September 1, 2010, through August 31, 2011) indicated the following high risk findings: a) no enterprise-wide solution in effect for encryption of Institutional laptops and mobile computing devices; b) workforce members are downloading ePHI, confidential, and restricted confidential information and other sensitive data onto portable computing devices for use outside the Institution.
12. MD Anderson failed to adequately remediate and manage its high risk findings though encryption, as required by the 45 C.F.R. § 164.312(a)(2)(iv) and its own policies, or, alternatively, document the reasons encryption was not feasible and implement an equivalent alternative measure to encryption from December 1, 2010, until at least January 25, 2013.[2]
13. Inasmuch as OCR's investigation indicated Security Rule noncompliance by MD Anderson, OCR attempted to reach a resolution of the matter by informal means during the period from approximately October 28, 2015, to August 11, 2016.
14. On August 11, 2016, OCR issued a Letter of Opportunity and informed MD Anderson that OCR's investigation indicated that MD Anderson failed to comply with the Privacy and Security Rules and that this matter had not been resolved by informal means despite OCR's attempts to do so. The letter stated that pursuant to 45 C.F.R. §

---

[1] *See* January 25, 2013 and January 10, 2014 letters from Baker Hostetler attorney Lynn Sessions to OCR Equal Opportunity Specialist Eva Lee.

[2] Although MD Anderson had yet to achieve a complete rate of encryption as required by 45 C.F.R.§164.312(a)(2)(iv), OCR determined to end the non-compliance period for this violation on January 25, 2013 in recognition of encryption of its managed computer inventory as of that date.

160.312(a)(3), OCR was informing MD Anderson of the preliminary indications of non-compliance and providing MD Anderson with an opportunity to submit written evidence of mitigating factors under 45 C.F.R. § 160.408 or affirmative defenses under 45 C.F.R. § 160.410 for OCR's consideration in making a determination of a CMP pursuant to 45 C.F.R. § 160.404. The letter stated that MD Anderson could also submit written evidence to support a waiver of a CMP for the indicated areas of non-compliance. Each of MD Anderson's indicated acts of noncompliance were described in the letter. The letter was delivered to MD Anderson and received by MD Anderson's agent on August 12, 2016. MD Anderson responded to OCR's letter on or about September 12, 2016.

15. OCR has determined that the information and arguments submitted by MD Anderson do not support an affirmative defense pursuant to 45 C.F.R. § 160.410. *See* Section IV below. OCR considered MD Anderson's response citing mitigating factors pursuant to 45 C.F.R. § 160.408 in determining the amount of the CMP indicated below. *See* Section V below. OCR has determined that the information and arguments submitted by MD Anderson do not support a waiver of the CMP pursuant to 45 C.F.R. § 160.412. *See* Section VI below.
16. OCR obtained the authorization of the Attorney General of the United States prior to issuing this Notice of Proposed Determination to impose a CMP.

III. Basis for CMP

Based on the above findings of fact, we have determined that MD Anderson is liable for the following violations of the HIPAA Rules and, therefore, is subject to a CMP.

1. MD Anderson failed to implement access controls – encryption and decryption, or an equivalent alternative measure, as required by 45 C.F.R. § 164.312(a)(2)(iv). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

    a. Calendar Year 2011 – 283 days, from March 24 through December 31 (maximum penalty of $1,500,000).
    b. Calendar Year 2012 – 366 days, from January 1 through December 31 (maximum penalty of $1,500,000).
    c. Calendar Year 2013 – 25 days, from January 1 through January 25, 2013 (maximum penalty of $1,500,000).

2. MD Anderson impermissibly disclosed the PHI of at least 34,883 individuals, in violation of 45 C.F.R. § 164.502(a). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

a. Number of individuals whose ePHI was impermissibly disclosed in 2012 due to April 30, 2012 theft of laptop and July 13, 2012 loss of an unencrypted USB thumb drive: 31,285 (maximum penalty of $1,500,000).
b. Number of individuals whose ePHI was impermissibly disclosed in 2013 due to December 2, 2013 loss of an unencrypted USB thumb drive: 3,598 (maximum penalty of $1,500,000).

IV. No Affirmative Defenses

By its letter of August 11, 2016, OCR offered MD Anderson the opportunity to provide written evidence of mitigating factors or affirmative defenses and/or its written evidence in support of a waiver of a CMP within thirty (30) days from the date of receipt of that letter. By letter dated September 12, 2016, MD Anderson submitted its response to OCR's August 11, 2016, letter. OCR has determined that the information contained therein did not provide a sufficient basis for an affirmative defense to the findings of violations pursuant to 45 C.F.R. § 160.410.

Specifically, with respect to each of the violations, MD Anderson did not correct the violation within a 30-day period from the first date that it knew, or, by exercising reasonable diligence, would have known of the violations. *See* 45 C.F.R. § 160.410(c)(2).

V. Factors Considered in Determining the Amount of the CMP

In determining the amount of the CMP, OCR has considered the following factors in accordance with 45 C.F.R. § 160.408.

In MD Anderson's response to August 11, 2016 OCR's Letter of Opportunity, it notes that the CMP should be mitigated because the alleged encryption noncompliance did not result in any known physical, financial, or reputational harm to any individuals nor did it hinder any individual's ability to obtain health care. OCR has considered this, and as a result, concludes that, despite the fact that it could impose a penalty of up to $50,000 a day for each day that MD Anderson was out of compliance with 45 C.F.R. § 164.312(a)(2)(iv), OCR proposes that the daily penalty amount of $2,000 per day be applied for these violations that were due to reasonable cause and not willful neglect under 45 C.F.R. § 160.404(b)(2)(ii)(A), specifically the encryption violations for which MD Anderson had abundant notice given the small breaches it reported beginning in 2011.

Each factor listed below was considered an aggravating factor in determining the amount of the CMP:

- The amount of time that MD Anderson continued to use unencrypted devices even after it had actual knowledge that encryption was necessary to ensure the security of ePHI. Specifically, the evidence

indicates that MD Anderson workforce members were using unencrypted devices to store ePHI as late as 2012 even after MD Anderson was on notice years earlier that its security program lacked encryption for protecting health information.

- MD Anderson's Information Security Program and Annual Reports for calendar years 2010-2011 identified encryption of confidential data on mobile media as a key risk area that is "currently not mitigated."

- MD Anderson's Corporate Compliance Risk Analysis for fiscal year 2011 (September 1, 2010, through August 31, 2011) indicated the following high risk findings: a) no enterprise-wide solution in effect for encryption of Institutional laptops and mobile computing devices; b) workforce members are downloading ePHI, confidential, and restricted confidential information and other sensitive data onto portable computing devices for use outside the Institution.

- MD Anderson submitted a series of breach reports to OCR on February 23, 2012, which indicated that, on nineteen occasions in 2011, Blackberry mobile devices containing ePHI were reported as lost or stolen to the University of Texas Police Department.

Therefore, OCR proposes the penalty amount of $2,000 per day for the violations of the encryption implementation specification (45 C.F.R. § 164.312(a)(2)(iv)) that were due to reasonable cause and not willful neglect under 45 C.F.R. § 160.404(b)(2)(ii)(A). However, based on the lack of evidence of harm to affected individuals, OCR continues to use the lowest amount in the reasonable cause tier, $1,000, for purposes of calculating the penalties for the impermissible disclosures violations (45 C.F.R. § 164.502(a)).

VI. Waiver

OCR has determined that there is no basis for waiver of the proposed CMP amount as set forth at 45 C.F.R. § 160.412. MD Anderson presented no evidence that the payment of the CMP would be excessive relative to the violations found here and described in OCR's letter to MD Anderson of August 11, 2016.

VII. Amount of CMP

A. Amount of CMP Per Violation

Based on the above factors, OCR finds that MD Anderson is liable for the following CMPs for each violation described in Section III:

1. Access controls – encryption and decryption (45 C.F.R. § 164.312(a)(2)(iv)): The CMP is $1,348,000 (see attached chart). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).

2. Impermissible disclosures (45 C.F.R. § 164.502(a)): $3,000,000 (see attached chart). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).

B. Total Amount of CMP

The total amount of CMPs for which OCR finds MD Anderson liable with regard to the violations described in Section III is $4,348,000 (see attached chart).

VIII. Right to a Hearing

MD Anderson has the right to a hearing before an administrative law judge to challenge these proposed CMPs. To request a hearing to challenge this proposed CMP, you must mail a request, via certified mail with return receipt request, under the procedures set forth at 45 C.F.R. Part 160 within 90 days of your receipt of this letter. Such a request must: (1) clearly and directly admit, deny, or explain each of the findings of fact contained in this notice; and (2) state the circumstances or arguments that you allege constitute the grounds for any defense, and the factual and legal basis for opposing the proposed CMPs. *See* 45 C.F.R. § 160.504(c). If you wish to request a hearing, you must submit your request to:

Karen Robinson, Esquire
Chief, Civil Remedies Division
Departmental Appeals Board, MS 6132
330 Independence Ave, SW
Cohen Building, Room G-644
Washington, D.C. 20201
Telephone: (202) 565-9462

Copy to:
Iliana Peters, Senior Advisor
Office for Civil Rights
200 Independence Avenue, SW
Suite 523E
Hubert H. Humphrey Building
Washington, D.C. 20201
Telephone: (202) 205-5704

A failure to request a hearing within 90 days permits the imposition of the proposed CMPs without a right a hearing under 45 C.F.R. § 160.504 or a right of appeal under 45 C.F.R. § 160.548. If you choose not to contest this

proposed CMP, you should submit a written statement accepting its imposition within 90 days of receipt of this notice.

If MD Anderson does not request a hearing within 90 days, then OCR will notify you of the imposition of the CMPs through separate letter, including instructions on how you may make payment, and the CMPs will become final upon receipt of such notice.

If you have any questions concerning this letter, please contact Roger C. Geer, Assistant Regional Counsel, at (214) 767-3450 or Roger.Geer@hhs.gov.

Sincerely,

[redacted]

Marisa M. Smith, Ph.D.
Regional Manager

Enclosure – CMP Penalty Chart

cc:
Dr. Ronald DePinho, President
The University of Texas MD Anderson Cancer Center
1515 Holcombe Blvd.
Houston, TX 77030