DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Voice - (214) 767-4056, (800) 368-1019
TDD - (214) 767-8940, (800) 537-7697
Fax - (214) 767-0432
http://www.hhs.gov/ocr

Office for Civil Rights, Southwest Region
1301 Young Street, Suite 1169
Dallas, TX 75202

Via Certified Mail Return Receipt Requested #70032260000698270976

September 30, 2016

Mr. David Berry
President, System Clinical Operations
Children's Medical Center
1935 Medical District Drive
Dallas, TX 75235

And Via E-mail: david.berry @childrens.com

RE: OCR Transaction Numbers 10-107242 and 13-162366

NOTICE OF PROPOSED DETERMINATION

Dear Mr. Berry:

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 $3,217,000 against Children's Medical Center (Children's).

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 CFR 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. Children's 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. Children's is headquartered in Dallas, Texas and operates three hospitals and numerous clinics in North Texas, including Children's Medical Center Dallas, the main hospital campus of Children's.
3. Children's creates, maintains, receives and transmits protected health information (PHI) related to its patients who receive health care services from workforce members of Children's.
4. On January 18, 2010, Children's filed a HIPAA Breach Notification Report with OCR in which it reported the loss of an unencrypted, non-password protected BlackBerry device at the Dallas/Fort Worth International Airport on November 19, 2009. Children's reported the device contained the electronic protected health information (ePHI) of approximately 3,800 individuals. OCR notified Children's, in writing, of its commencement of an investigation of this breach report and of Children's compliance with the Privacy, Security and Breach Notification Rules on or about June 14, 2010.
5. During the course of OCR's investigation, Children's submitted a Security Gap Analysis and Assessment conducted for Children's December 2006 - February 2007 by Strategic Management Systems, Inc. (SMS) (SMS Gap Analysis). The SMS Gap Analysis identified the absence of risk management as a major finding and recommended that Children's implement encryption to avoid loss of PHI on stolen or lost laptops.

6. In August 2008, PricewaterhouseCoopers (PwC) conducted a separate analysis of threats and vulnerabilities to certain ePHI (PwC Analysis) for Children's and determined that encryption was necessary and appropriate. The PwC Analysis also determined that a mechanism was not in place to protect data on a laptop, workstation, mobile device, or USB thumb drive if the device was lost or stolen and identified the loss of data at rest through unsecured mobile devices as being "high" risk. PwC identified data encryption as a "high priority" item and recommended that Children's implement data encryption in the fourth quarter of 2008.
7. As a result of its receipt of the 2007 SMS Gap Analysis and 2008 PwC Analysis, Children's had actual knowledge of the risks to unencrypted ePHI at rest by at least March 2007, at least one year prior to the reported security incidents. Appropriate commercial encryption products were available to achieve encryption of laptops, workstations, mobile devices, and USB thumb drives in use by Children's staff by, at least, the time of the PwC Analysis in 2008; however, Children's had not implemented encryption on all devices as of April 9, 2013.
8. Despite the findings of SMS and PwC and Children's actual knowledge about the risk of maintaining unencrypted ePHI on its devices, Children's issued unencrypted BlackBerry devices to nurses beginning in 2007 and allowed its workforce members to continue using unencrypted laptops and other mobile devices until at least April 9, 2013.
9. The HIPAA regulation at 45 C.F.R. § 164.306(d)(3) requires a covered entity to implement "addressable" implementation specifications if such implementation is reasonable and appropriate. If implementation is not reasonable and appropriate, the covered entity must document why it would not be reasonable and appropriate and must implement an equivalent alternative measure, if reasonable and appropriate. Children's failed to appropriately document its decision to not implement encryption on mobile devices and/or any applicable rationale behind a decision to use alternative security measures to encryption. Children's did not implement security measures that were an equivalent alternative to the security protection available from encryption solutions as recommended by the 2007 SMS Gap Analysis and the 2008 PwC Analysis.
10. Prior to at least November 9, 2012, Children's did not implement sufficient policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within the facility.
11. Children's was unable to identify all devices to which the device and media control policy should apply prior to completing a full-scope inventory to identify all information systems containing ePHI in November 9, 2012. Prior to November 2012, Children's information technology (IT) assets were inventoried and managed separately from the inventory of devices used within its Biomedical Department. Children's IT asset policies did not apply to devices that accessed or stored ePHI that were managed by the Biomedical Department. As Children's did not conduct a complete inventory to identify all devices to which its IT asset policies apply to ensure that all devices were covered by its device and media control policies, Children's was out of compliance with the Security Rule at 45 C.F.R. § 164.310(d)(1).

12. In a letter dated August 22, 2011, from Children's Vice President of Compliance and Internal Audit and Chief Compliance Officer Ron Skillens to OCR Equal Opportunity Specialist Jamie Sorley, Mr. Skillens stated that a Children's workforce member (an unidentified medical resident) lost an iPod device in December 2010. The iPod had been synched to the resident's Children's email account, which resulted in the ePHI of at least 22 individuals being placed on the device. The ePHI on the iPod was not encrypted. The loss of the iPod resulted in the impermissible disclosure of ePHI by the medical resident. The ePHI of 22 individuals was impermissibly disclosed, because the workforce member and agent of Children's provided access to any unauthorized person who discovered the device.
13. In September 2012, the HHS Office of the Inspector General (OIG) issued the findings from its audit of Children's that focused on information technology controls for devices such as smartphones and USB drives. Among other things, the report, entitled "Universal Serial Bus Control Weaknesses Found at Children's Medical Center," found that Children's had insufficient controls to prevent data from being written onto unauthorized and unencrypted USB devices and that "without sufficient USB controls, there was a risk that ePHI could have been written onto an unauthorized/unencrypted USB device and taken out of the hospital, resulting in a data breach." A copy of this report was provided to Mr. Skillens.
14. On July 5, 2013, Children's filed a separate HIPAA Breach Notification Report with OCR, reporting the theft of an unencrypted laptop from its premises sometime between April 4 and April 9, 2013. Children's reported the device contained the ePHI of 2,462 individuals. OCR notified Children's, in writing, of its commencement of an investigation of this breach report and of Children's compliance with the Privacy, Security and Breach Notification Rules on or about July 11, 2013.
15. In Children's July 5, 2013, Breach Report referenced above, Children's reported to OCR that, sometime between April 4 and April 9, 2013, a password-protected, unencrypted laptop, was stolen from an operating room storage area. Although Children's implemented some physical safeguards to the operating room storage area (*e.g.*, badge access was required, and a security camera was present at one of the entrances), it also provided access to the area to staff who were not authorized to access ePHI. Children's provided janitorial staff with unrestricted access to the area where the laptop was stored but did not provide encryption to protect the ePHI of this laptop from access by such unauthorized persons; Children's internal investigation concluded that the laptop was probably stolen by a member of the janitorial staff.
16. The theft of the laptop resulted in the impermissible disclosure of ePHI. The ePHI of at least 2,462 individuals was impermissibly disclosed because a workforce member and agent of Children's provided access to any unauthorized person who gained possession of this this laptop with unencrypted ePHI.
17. Inasmuch as OCR's investigation indicated Privacy and Security Rule noncompliance by Children's, OCR attempted to reach a resolution of the matter by informal means during the period from approximately November 6, 2015, to August 30, 2016.

18. On May 10, 2016, OCR issued a Letter of Opportunity and informed Children's that OCR's investigation indicated that Children's 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. § 160.312(a)(3), OCR was informing Children's of the preliminary indications of non-compliance and providing Children's 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 Children's could also submit written evidence to support a waiver of a CMP for the indicated areas of non-compliance. Each of Children's indicated acts of noncompliance and the potential CMP for them were described in the letter. The letter was delivered to Children's and received by Children's agent on May 12, 2016. Children's responded to OCR's letter on or about June 9, 2016.
19. OCR has determined that the information and arguments submitted by Children's do not support an affirmative defense pursuant to 45 C.F.R. § 160.410. (*See* Section IV below). OCR considered Children'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 Children's do not support a waiver of the CMP pursuant to 45 C.F.R. § 160.412. (*See* Section VI below).
20. 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 Children's is liable for the following violations of the HIPAA Rules and, therefore, is subject to a CMP.

1. Children's 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). Further, Children's failed to document its decision not to implement encryption or an equivalent alternative measure and the rationale behind that decision, as required by 45 C.F.R. § 164.306(d)(3), respectively. OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

    a. Calendar Year 2010 – 93 days, from September 30 through December 31 (maximum penalty of $1,500,000)

    b. Calendar Year 2011 – 365 days, from January 1 through December 31 (maximum penalty of $1,500,000))

    c. Calendar Year 2012 – 366 days, from January 1 through December 31 (maximum penalty of $1,500,000)

    d. Calendar Year 2013 – 99 days, from January 1 through April 9 (maximum penalty of $1,500,000)

2. Children's failed to implement sufficient policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within the facility, as required by 45 C.F.R. §

164.310(d)(1). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

a. Calendar Year 2010 – 93 days, from September 30 through December 31 (maximum penalty of $1,500,000)

b. Calendar Year 2011 – 365 days, from January 1 through December 31 (maximum penalty of $1,500,000))

c. Calendar Year 2012 – 314 days, from January 1 through November 9 (maximum penalty of $1,500,000)

3. Children's impermissibly disclosed the PHI of at least 2,484 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 due to December, 2010 loss of iPod- 22 (maximum penalty of $1,500,000).

b. Number of individuals whose ePHI was impermissibly disclosed due to April 9, 2013 theft of laptop- 2,462 (maximum penalty of $1,500,000).

IV. No Affirmative Defenses

By its letter of May 10, 2016, OCR offered Children's 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 June 9, 2016, Children's submitted its response to OCR's May 10, 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 after February 18, 2009, Children's 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, we have considered the following factors in accordance with 45 C.F.R. § 160.408.

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

(A) The amount of time that Children's continued to use unencrypted devices even after it had actual knowledge that encryption was necessary to ensure the security of ePHI.

1. The 2008 PwC Analysis, which specifically determined that encryption was necessary and appropriate and that a mechanism was not in place to protect data on a laptop, workstation, mobile device, or USB thumb drive, if the device was lost or stolen, and identified the loss of data at rest through unsecured mobile devices as being "high" risk.

2. The September 2012 HHS OIG Report, which recommended that Children's develop and implement technical controls for all of its computer platforms to prevent ePHI from being written onto unauthorized/unencrypted devices.

(B) Children's prior history of non-compliance with the Privacy and Security Rules.

1. During the investigation, Children's acknowledged that additional devices with unsecured ePHI had been stolen prior to the implementation of the Breach Notification Rule: a laptop in February 2008; a laptop in October 2008; and a Blackberry in July 2009. These losses put Children's on definitive notice of the active risk of compromise to ePHI on its devices and of its noncompliance with the Privacy and Security Rules.
2. Children's 2010 Breach Notification Report involving the loss of an unencrypted, non-password protected Blackberry device containing ePHI of approximately 3,800 individuals evidences noncompliance with the same or similar provisions of the Privacy and Security Rules that resulted in the 2013 breach that gives rise to the violations that form the basis for the instant CMP.
3. Children's subsequently reported the loss of an additional mobile device containing unsecured ePHI, an iPod lost in December 2010. This incident again involved the same or similar provisions of the Privacy and Security Rules and further evidences Children's extended noncompliance.

In consideration of Children's assertion 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 proposes the minimum penalty amount of $1,000 per day for the violations that were due to reasonable cause and not willful neglect under 45 C.F.R. § 160.404(b)(2)(ii)(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. Children's 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 Children's of May 10, 2016.

VII. Amount of CMP

A. Amount of CMP Per Violation

Based on the above factors, OCR finds that Children's 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 $ 923,000 (see attached chart). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).

2. Device and media controls (45 C.F.R. § 164.310(d)(1)): The CMP is $ 772,000 (see attached chart). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).

3. Impermissible disclosures (45 C.F.R. § 164.502(a)): $1,522,000. 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 Children's liable with regard to the violations described in Section III is $3,217,000 (see attached chart).

VIII. Right to a Hearing

Children's 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 Children's 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,

Marisa M. Smith, Ph.D.
Regional Manager

Enclosure – CMP Penalty Chart

cc:
Mr. Theodore Kobus III
Baker and Hostetler
45 Rockefeller Plaza
New York, New York 10111
Via email: tkobus@bakerlaw.com

Mr. Richard Roper
Thompson & Knight, LLP
One Arts Plaza
1722 Routh Street, Suite 1500
Dallas, Texas 75201
Via email: richard.roper@tklaw.com

Childrens Medical Center of Dallas

10-107242 - July 2010 Breach
13-162366 - April 2013 Breach

NPD issuance date of 9/30/2016

Regulatory Provision	Post-HITECH Penalty Tier	Beginning Date	End Date	Variable (Nature of Violation)	# of Violations	Amount Per Violation	Potential Penalty	Applicable Calendar Year Cap	Adjusted Total
Access Controls (Encryption):									
45 C.F.R. § 164.312(a)(2)(iv)	Reasonable cause								
		9/30/2010	12/31/2010	Daily	93	$ 1,000	$ 93,000	$ 1,500,000	$ 93,000
		1/1/2011	12/31/2011	Daily	365	$ 1,000	$ 365,000	$ 1,500,000	$ 365,000
		1/1/2012	12/31/2012	Daily	366	$ 1,000	$ 366,000	$ 1,500,000	$ 366,000
		1/1/2013	4/9/2013	Daily	99	$ 1,000	$ 99,000	$ 1,500,000	$ 99,000
								total	**$ 923,000**
Device and Media Controls:									
45 C.F.R. § 164.310(d)(1)	Reasonable cause	9/30/2010	12/31/2010	Daily	93	$ 1,000	$ 93,000	$ 1,500,000	$ 93,000
		1/1/2011	12/31/2011	Daily	365	$ 1,000	$ 365,000	$ 1,500,000	$ 365,000
		1/1/2012	11/9/2012	Daily	314	$ 1,000	$ 314,000	$ 1,500,000	$ 314,000
								total	**$ 772,000**
Impermissible Disclosure:									
45 C.F.R. §164.502(a)	Reasonable Cause	12/19/2010	12/19/2010	one time	22	$1,000	$22,000	$ 1,500,000	$22,000
45 C.F.R. §164.502(a)	Reasonable Cause	4/9/2013	4/9/2013	one time	2,462	$1,000	$2,462,000	$ 1,500,000	$1,500,000
								total	**$1,522,000**
								grand total=	**$3,217,000**