DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Voice - (800) 368-1019
TDD - (214) 767-8940
FAX - (214) 767-0432
http://www.hhs.gov/ocr/

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

Via USPS Certified Mail
Return Receipt Requested

July 29, 2019

Texas Health and Human Services Commission
Dr. Courtney N. Phillips, Executive Commissioner
4900 N. Lamar Blvd.
Austin, TX 78751-2316

Re: OCR Transaction Number: 15-213170

NOTICE OF PROPOSED DETERMINATION

Dear Dr. Phillips:

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), I am writing to inform you that OCR is proposing to impose a civil money penalty (CMP) of $1,600,000 against the Texas Health and Human Services Commission (HHSC), Department of Aging and Disability Services.[1]

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, 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 authority includes violations of the applicable provisions of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules)

[1] As of September 1, 2017, the functions of the Texas Department of Aging and Disability Services (DADS) were transferred to the Texas Health and Human Services Commission (HHSC), and DADS was abolished. Because of this transfer and the abolishment of DADS, the covered entity will be referred to as HHSC throughout this Notice. The CMP reflects the penalty tiers described in the Notification of Enforcement Discretion (April 30, 2019). See https://www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties.

and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D), 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 $25,000.

- 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 $100,000. 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 $250,000.

- 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.

- As required by law, OCR has adjusted the CMP ranges and calendar year cap for each penalty tier for inflation.[2] The adjusted amounts are applicable only to CMPs whose violations occurred after November 2, 2015.

OCR is precluded from imposing a CMP unless the action is commenced within six years from the date of the violation.[3]

II. Findings of Fact

1. HHSC 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] See Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Sec. 701 of Public Law 114-74.
[3] 45 C.F.R. § 160.104

2. HHSC is a Texas state agency headquartered in Austin, Texas. It is responsible for the delivery of benefits and services in Texas for the following programs, among others: Medicaid for families and children; long-term care for people who are older or who have disabilities; behavioral health services; and services for women and other people with special health needs. In addition, HHSC manages the day-to-day operations of state supported living centers and state hospitals. HHSC also oversees regulatory functions including licensing and credentialing long-term care facilities, such as nursing homes and assisted living facilities.

3. HHSC creates, maintains, receives, and transmits protected health information (PHI) related to its beneficiaries who receive health care benefits and services from HHSC.

4. HHSC submitted a Breach Notification Report ("Report") to OCR on June 11, 2015, notifying OCR that, on April 21, 2015, it discovered a security vulnerability in a web-facing application designed for the Community Living Assistance and Support Services and Deaf Blind with Multiple Disabilities (CLASS/DBMD) program;[4] the CLASS/DBMD application was intended for collecting and reporting information regarding "Utilization Management and Review" activities to the Centers for Medicare & Medicaid Services (CMS) on the CLASS/DBMD waiver programs.

5. HHSC reported that, under the CMS waiver programs, it is required to collect waiver program performance data for CLASS and DBMD including applicant and enrollee community and institutional service choice, Level of Care, Plan of Care, and waiver provider choice. CMS requires HHSC to report this program performance information, as part of an evidentiary report on all §1915(c) waiver programs, approximately eighteen months prior to the waiver renewal date (every five years).

6. HHSC reported that the CLASS/DBMD application compromised electronic protected health information (ePHI) by allowing an undetermined number of unauthorized users to view the ePHI without verifying user credentials. HHSC learned of the breach from an unauthorized user who accessed ePHI in the application without being required to input user credentials.

7. OCR initiated a compliance review of HHSC on June 23, 2015.

8. In its August 31, 2015, response to OCR's Data Request dated July 23, 2015, HHSC acknowledged that the CLASS/DBMD application contained the names, residences, addresses, Social Security and Medicaid numbers, and treatment or diagnosis information of 6,617 individuals.

[4] Community Living Assistance and Support Services (CLASS) and Deaf Blind with Multiple Disabilities Program (DBMD) are home and community based services operated by the State of Texas as alternatives to institutional placement for individuals with a specific disabilities. These waiver programs are authorized at 42 U.S.C. 1396n, §1915(c) of the Social Security Act.

9. As set forth in 45 C.F.R. § 164.502(a), a covered entity may not use or disclose protected health information except as permitted or required by the HIPAA Privacy Rule.

10. HHSC impermissibly disclosed the ePHI of 6,617 individuals when HHSC placed the CLASS/DBMD application on their public server.

11. The HIPAA Security Rule at 45 C.F.R. § 164.312(a)(1) requires a covered entity to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

12. The web-based CLASS/DBMD application did not require the user to input any access credentials prior to accessing or viewing the ePHI.

13. By placing the CLASS/DBMD application on their public server without requiring users to provide access credentials, HHSC failed to implement access controls on all of its systems and applications throughout its enterprise in violation of 45 C.F.R. § 164.312(a)(1).

14. The HIPAA Security Rule at 45 C.F.R. § 164.312(b) requires a covered entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

15. In its June 23, 2015 Data Request, OCR requested that HHSC provide a copy of its current HIPAA administrative and technical policies and procedures.

16. HHSC provided no evidence that the application was capable of auditing user access after it was moved to the unsecure public server as required by 45 C.F.R. § 164.312(b).

17. HHSC failed to implement audit controls to all of its systems and applications, like the application involved in the breach, as required by 45 C.F.R. § 164.312(b).

18. The HIPAA Security Rule at 45 C.F.R. § 164.308(a)(1)(ii)(A) requires a covered entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by a covered entity.

19. In its August 31, 2015, response to OCR's Data Request dated July 23, 2015, HHSC acknowledged that, while it had performed "risk assessment activities" on individual applications and servers, it had never performed an "agency-wide" security risk analysis.

20. On July 28, 2017, OCR received documentation, which HHSC purported to be DADS' risk analysis.

21. On May 23, 2018, OCR issued a Letter of Opportunity and informed HHSC that OCR's investigation indicated that HHSC 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 HHSC of the preliminary indications of non-compliance and providing HHSC 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 HHSC could also submit written evidence to support a waiver of a CMP for the indicated areas of non-compliance. Each of HHSC's indicated acts of noncompliance were described in the letter.

22. The Letter of Opportunity was delivered to HHSC and received by HHSC's agent on May 24, 2018.

23. In response to OCR's Letter of Opportunity, received by HHSC on May 24, 2018, HHSC did not provide any 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. HHSC also did not submit any written evidence to support a waiver of a CMP for the indicated areas of non-compliance.

24. 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 HHSC is liable for the following violations of the HIPAA Rules and, therefore, is subject to a CMP.

1. HHSC impermissibly disclosed the PHI of at least 6,617 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.

   Number of individuals whose ePHI was impermissibly disclosed in 2015 due to placing a web application on its public server that permitted unauthorized users to view ePHI without verifying user credentials – 6,617 (maximum penalty of $100,000).

2. HHSC failed to implement access controls—requiring users to provide credentials to gain access to ePHI contained in the CLASS/DBMD application —as required by 45 C.F.R. § 164.312(a)(1). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

a. Calendar Year 2013- 156 days from July 29 to December 31 (maximum penalty of $100,000).

b. Calendar Year 2014- 365 days from January 1 to December 31 (maximum penalty of $100,000).

c. Calendar Year 2015- 306 days from January 1 to November 2 (maximum penalty of $100,000).

d. Calendar Year 2015- 59 days from November 3 to December 31 (maximum penalty of $100,000).

e. Calendar Year 2016- 366 days from January 1 to December 31 (maximum penalty of $100,000).

f. Calendar Year 2017- 243 days from January 1 to August 31 (maximum penalty of $100,000).

3. HHSC failed to implement audit controls—ensuring that the CLASS/DBMD application was capable of auditing user access after it was moved to the unsecure public server—as required by 45 C.F.R. § 164.312(b). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

a. Calendar Year 2013 - 156 days from July 29 to December 31 (maximum penalty of $100,000).

b. Calendar Year 2014 - 365 days from January 1 to December 31 (maximum penalty of $100,000).

c. Calendar Year 2015 - 306 days from January 1 to November 2 (maximum penalty of $100,000).

d. Calendar Year 2015 - 59 days from November 3 to December 31 (maximum penalty of $100,000).

e. Calendar Year 2016 - 366 days from January 1 to December 31 (maximum penalty of $100,000).

f. Calendar Year 2017 - 243 days from January 1 to August 31 (maximum penalty of $100,000).

4. HHSC failed to perform an accurate, thorough, and enterprise-wide risk analysis that meets the requirements of 45 C.F.R. § 164.308(a)(1)(ii)(a). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

a. Calendar Year 2013 - 156 days from July 29 to December 31 (maximum penalty of $100,000).

b. Calendar Year 2014 - 365 days from January 1 to December 31 (maximum penalty of $100,000).

c. Calendar Year 2015 - 306 days from January 1 to November 2 (maximum penalty of $100,000).

d. Calendar Year 2015 - 59 days from November 3 to December 31 (maximum penalty of $100,000).

e. Calendar Year 2016 - 366 days from January 1 to December 31 (maximum penalty of $100,000).

f. Calendar Year 2017 - 209 days from January 1 to July 28, 2017 (maximum penalty of $100,000).

IV. No Affirmative Defenses

By its letter of May 23, 2018, OCR offered HHSC 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. HHSC did not submit any 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.

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.

OCR notes that HHSC's noncompliance with regulations referenced above 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 and HHSC immediately removed the application once it received a report that unauthorized users could access the ePHI of individual beneficiaries. 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 HHSC was out of compliance with these regulations, OCR proposes that the daily penalty amount of $1,000 per day ($1,141 after November 2, 2015) 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).

However, in determining the amount of the CMP, OCR considered the amount of time that HHSC continued to remain out of compliance with 45 C.F.R. § 164.308(a)(1)(ii)(a) an aggravating factor.

Specifically, the evidence indicates that, in its August 31, 2015, Data Request Response to OCR, HHSC committed to remediate its failure to perform a Security Risk Analysis by undertaking and completing an agency wide analysis by August 31, 2016, as required by 45 C.F.R. § 164.308(a)(1)(ii)(a). However, HHSC failed to do so. OCR proposes that the daily penalty amount of $1,000 per day ($1,141 after November 2, 2015) 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).

Therefore, based on the lack of evidence of harm to affected individuals and the prompt removal of the flawed CLASS/DBMD application upon discovery of the disclosures, OCR continues to use the lowest amount in the reasonable cause tier, $1,000 ($1,141 after November 2, 2015), for purposes of calculating the penalties for violations under 45 C.F.R. § 164.502(a) (impermissible disclosures), 45 C.F.R. § 164.312(b) (audit controls) and 45 C.F.R. § 164.312(a)(1) (access control).

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. HHSC 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 HHSC of May 23, 2018.

VII. Amount of CMP

A. Amount of CMP Per Violation

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

1. Impermissible disclosures – (45 C.F.R. § 164.502(a)): The CMP is $100,000 (see attached chart). This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).
2. Access controls – (45 C.F.R. § 164.312(a)(1): The CMP is $500,000. This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).
3. Audit controls – (45 C.F.R. § 164.312(b): The CMP is $500,000. This CMP amount is based on 45 C.F.R. § 160.404(b)(2)(ii).
4. Risk analysis - 45 C.F.R. § 164.308(a)(1)(ii)(a): The CMP is $500,000 (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 HHSC liable with regard to the violations described is $1,600,000.

VIII. Right to a Hearing

HHSC has the right to a hearing before an administrative law judge to challenge these proposed CMPs. To request a hearing to challenge these proposed CMPs, 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:
Serena Mosley-Day, 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 to 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 HHSC does not request a hearing within 90 days, then OCR will notify you of the imposition of the CMPs through a 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

Marisa M. Smith, Ph.D.
Regional Manager

Enclosure – CMP Penalty Chart

	HHSC/DADS									
	15-213170									
1	Impermissible Disclosure:									
	45 C.F.R. § 164.502(a)	Reasonable cause								
				4/21/2015	one time	6617	$ 1,000	$ 6,617,000	$ 100,000	$ 100,000
2	Risk Analysis									
	45 C.F.R. § 164.308(a)(1)(ii)(A)	Reasonable cause								
			7/29/2013	12/31/2013	Daily	156	$ 1,000	$ 156,000	$ 100,000	$ 100,000
			1/1/2014	12/31/2014	Daily	365	$ 1,000	$ 365,000	$ 100,000	$ 100,000
			1/1/2015	11/2/2015	Daily	306	$ 1,000	$ 306,000	$ 100,000	$ 100,000
		*inflation adjustment	11/3/2015	12/31/2015	Daily	59	$ 1,141	$ 67,319	$ 100,000	
			1/1/2016	12/31/2016	Daily	366	$ 1,141	$ 417,606	$ 100,000	$ 100,000
			1/1/2017	7/28/2017	Daily	209	$ 1,141	$ 238,469	$ 100,000	$ 100,000
3	Access Controls									
	45 C.F.R. § 164.312(a)(1)	Reasonable cause								
			7/29/2013	12/31/2013	Daily	156	$ 1,000	$ 156,000	$ 100,000	$ 100,000
			1/1/2014	12/31/2014	Daily	365	$ 1,000	$ 365,000	$ 100,000	$ 100,000
			1/1/2015	11/2/2015	Daily	306	$ 1,000	$ 306,000	$ 100,000	$ 100,000
		*inflation adjustment	11/3/2015	12/31/2015	Daily	59	$ 1,141	$ 67,319	$ 100,000	
			1/1/2016	12/31/2016	Daily	366	$ 1,141	$ 417,606	$ 100,000	$ 100,000
			1/1/2017	8/31/2017	Daily	243	$ 1,141	$ 277,263	$ 100,000	$ 100,000
4	Audit controls									
	45 C.F.R. § 164.312(b)	Reasonable cause								
			7/29/2013	12/31/2013	Daily	156	$ 1,000	$ 156,000	$ 100,000	$ 100,000
			1/1/2014	12/31/2014	Daily	365	$ 1,000	$ 365,000	$ 100,000	$ 100,000
			1/1/2015	11/2/2015	Daily	306	$ 1,000	$ 306,000	$ 100,000	$ 100,000
		*inflation adjustment	11/3/2015	12/31/2015	Daily	59	$ 1,141	$ 67,319	$ 100,000	
			1/1/2016	12/31/2016	Daily	366	$ 1,141	$ 417,606	$ 100,000	$ 100,000
			1/1/2017	8/31/2017	Daily	243	$ 1,141	$ 277,263	$ 100,000	$ 100,000
									grand total =	**$ 1,600,000**