IN THE CHANCERY COURT OF DAVIDSON COUNTY, TENNESSEE
FOR THE TWENTIETH JUDICIAL DISTRICT AT NASHVILLE

STATE OF TENNESSEE, *ex rel.* HERBERT H. SLATERY III, Attorney General and Reporter,

Plaintiff,

v.

CHS/COMMUNITY HEALTH SYSTEMS INC., a Delaware corporation, and CHSPSC, LLC, f/k/a COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, a Delaware corporation,

Defendants.

Case No. 20-1006-I

COMPLAINT

1. The State of Tennessee, by and through Herbert H. Slatery III, Attorney General and Reporter, brings this civil law enforcement action against CHS/Community Health Systems Inc. and CHSPSC, LLC, f/k/a Community Health Systems Professional Services Corporation, for violations of the Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101–131 and the Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to -2111, in connection with a data breach disclosed by Defendants in August 2014.

2. The State seeks injunctive relief, civil penalties, and other equitable and statutory relief as set forth below.

THE PARTIES

3. This action is brought for and on behalf of the State of Tennessee by Herbert H. Slatery III, Attorney General and Reporter, pursuant to the provisions of Tenn. Code Ann. §§ 47-

18-108 and -114, -2106, and his common law authority as Attorney General to represent the People of the State of Tennessee.

4. Plaintiff, the State of Tennessee, through Herbert H. Slatery III, Attorney General and Reporter, is charged with enforcing the Tennessee Consumer Protection Act of 1977 (TCPA), Tenn. Code Ann. §§ 47-18-101 to -131, which prohibits unfair or deceptive acts or practices affecting the conduct of any trade or commerce, and the Tennessee Identity Theft Deterrence Act of 1999 (TITDA), Tenn. Code Ann. §§ 47-18-2101 to -2111, which mandates the use of reasonable efforts to protect social security numbers from public disclosure. The Attorney General may initiate civil law enforcement proceedings in the name of the State to enjoin violations of the TCPA and TITDA, and to secure such equitable and other relief as may be appropriate in each case under broad grants of statutory authority in accordance with Tenn. Code Ann. §§ 8-6-109 and 47-18-108(a)(1), and -2106.

5. The State has reason to believe that Defendants have violated the TCPA by engaging in unfair and deceptive acts or practices in whole or in part in Tennessee, has violated TITDA by failing to use reasonable efforts to protect social security numbers of Tennessee residents from public disclosure, and that this enforcement action is in the public interest.

6. Defendant CHS/Community Health Systems, Inc. (CHS/CHSI) is a Delaware publicly traded company with its principal place of business at 4000 Meridian Blvd., Franklin, Tennessee 37067-6325 and is the parent company of Defendant CHSPSC, LLC. At all relevant times, CHS/CHSI conducted business in Tennessee.

7. Defendant CHSPSC, LLC (CHSPSC) is a Delaware limited liability company that provides management and professional services to various hospitals and other healthcare providers

affiliated with CHS/CHSI. Its principal place of business is 4000 Meridian Blvd., Franklin, Tennessee 37067.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to Tenn. Code Ann. §§ 47-18-108(a), 47-18-114, and 47-18-2106). Defendants are doing business in Tennessee and are also subject to the jurisdiction of the State's long-arm statutes, Tenn. Code Ann. §§ 20-2-214(a)(1), (2), (5), and (6), 20-2-223(a)(1), (2), (3), and (4), and 20-2-225.

9. Venue is proper in Davidson County pursuant to Tenn. Code Ann. § 47-18-108(a)(4) because it is one of the counties in which the alleged unfair and/or deceptive trade practices took place.

STATUTORY FRAMEWORK

10. The TCPA, Tenn. Code Ann. § 47-18-101 to -131, prohibits unfair and deceptive acts and practices in trade and commerce.

11. The acts described below in paragraphs 13-22 constitute unfair and deceptive acts and practices in trade and commerce.

ACTS OF AGENTS

12. Whenever in this Complaint it is alleged that Defendants did any act, it is meant that:

A. Defendants performed or participated in the act; or

B. Defendants' officers, affiliates, subsidiaries, divisions, agents or employees performed or participated in the act on behalf of and under the authority of the Defendants.

FACTS

13. CHS/CHSI and CHSPSC are headquartered at 4000 Meridian Blvd. in Franklin, Tennessee. CHSPSC provides services, including management, consultation, and information technology services for hospitals and other affiliates of CHS/CHSI. CHS/CHSI is one of the largest publicly-traded hospital companies in the United States and a leading operator of general acute-care hospitals in non-urban and mid-size markets throughout the country.

14. Prior to the breach, CHS/CHSI and CHSPSC, LLC (hereafter "Defendants") owned, leased or operated 206 affiliated hospitals in 29 states and these affiliates offered a broad range of health care services including inpatient and surgical services, outpatient treatment, and skilled nursing care.

Data Breach Experienced by Defendants

15. In August 2014, Defendants publicly disclosed that in the preceding month CHSPSC had confirmed that its computer network had been accessed by intruders, first in April and again in June of 2014.

16. Defendants further disclosed that they believed the intruder had used malware to gain access to the company's security systems and had successfully copied and transferred data, including the personal information of approximately 4.5 million patients that was on CHSPSC's systems. After additional investigation, Defendants disclosed that the total number of patients whose personal information was accessed was approximately 6.1 million. The data taken related to patients of some of Defendants' affiliated physician practices and clinics and included patients' names, addresses, birthdates, social security numbers, and in some cases telephone numbers as well as the names of employers or guarantors. However, to the best of Defendants' knowledge, no credit card information or medical or clinical information was taken.

17. Defendants also provided notice of the breach to government regulators and mailed notification letters to all affected patients informing them about the data breach. In these letters Defendants offered affected patients the opportunity to enroll in free identity theft protection and credit monitoring services. Defendants also established a toll-free number and website where affected patients could obtain additional information including how to access these services.

Defendants' Data Collection and Representations to Consumers

18. In the regular course of business, Defendants collect and maintain the personal information of individuals including individual names, addresses, dates of birth, and social security numbers.

19. Defendants also create, receive, use and maintain electronic Protected Health Information subject to the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.*, (collectively, HIPAA). HIPAA and its Rules require the implementation of appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. *See,* 45 CFR Part 160 and Subparts A and C of Part 164.

20. Through its various policies, including a Privacy Policy and website Terms of Use, Defendants disclosed to consumers that they collected personal information, and generally explained what information was collected and the purpose for which it was collected and used, and the circumstances in which such information might be disclosed. Defendants also provided patients with the Notice of Privacy Protections as required by the HIPAA Privacy Rule.

21. In their disclosures to consumers, Defendants represented that they protected personal information, specifically that they treated the "…technical side of security seriously [and] stored personal information … on a secure server in a way that maximizes security and confidentiality," and employed security measures to protect information from unauthorized disclosure through various means such as encryption.

22. Defendants engage in trade and commerce and do business in Tennessee at their headquarters, located at 4000 Meridian Blvd., Franklin, Tennessee 37067, in addition to at least nine locations where they provide healthcare services, including the following: Tennova Healthcare, Clarksville, in Montgomery County; Tennova Healthcare, Harton, located in Tullahoma, Coffee County; Tennova-LaFollette Medical Center, LaFollette, in Campbell County; Tennova-North Knoxville Medical Center, Powell, in Knox County; Tennova- Turkey Creek Medical Center, Knoxville, in Knox County; Tennova Healthcare-Cleveland, Cleveland, in Bradley County; Tennova-Jefferson Memorial Hospital, Jefferson City, in Jefferson County; Tennova-Newport Medical Center, Newport, in Cocke County; and Tennova Healthcare-Shelbyville, Shelbyville, in Bedford County.

VIOLATIONS OF THE LAW

COUNT I:
Tennessee Consumer Protection Act, Tenn. Code Ann. § 47–18–104(a) and (b)

23. Plaintiff, the State of Tennessee, incorporates by reference and re-alleges every allegation contained in paragraphs 1–22 of this Complaint.

24. Defendants' collection and retention of Tennessee consumers' personal information, and all representations made to consumers regarding Defendants' data security

practices regarding such personal information, as alleged herein, constitute "trade," "commerce," and/or "consumer transactions" as defined in Tenn. Code Ann. § 47-18-103(20).

25. By engaging in the following misleading or deceptive acts or practices, Defendants have violated Tenn. Code Ann. § 47-18-104(a), (b)(5), (b)(7), and (b)(27):

A. Defendants failed to implement and maintain reasonable security practices to protect consumers' personal information it collects and maintains;

B. Defendants failed to store personal information in a way that maximized its security and confidentiality; and

C. Defendants permitted the disclosure of Protected Health Information in a manner inconsistent with the requirements of HIPAA and its rules.

COUNT II
Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. §§ 47-18-2101 to -2111

26. Plaintiff, the State of Tennessee, incorporates by reference and re-alleges every allegation contained in paragraphs 1–22 of this Complaint.

27. Defendant CHSPSC collects the personal information of Tennessee consumers, including their social security numbers.

28. Defendant has violated the Tennessee Identity Theft Deterrence Act of 1999 (TITDA), Tenn. Code Ann. §§ 47-18-2110, by failing to implement reasonable efforts to protect Tennesseans' social security numbers from disclosure to the public. Specifically, Defendant CHSPSC failed to maintain reasonable security measures to protect records containing the social security numbers of Tennessee consumers from unauthorized access, use, modification or disclosure.

29. Defendant's failure to take reasonable steps to protect consumers' personal information also constitutes an unfair or deceptive trade practice that violates the TCPA pursuant to Tenn. Code Ann. § 47-18-2106.

PRAYER FOR RELIEF

Therefore, the State, pursuant to Tenn. Code Ann. § 47-18-108(a) and (b), -114, and -2106, and this Court's own equitable powers, respectfully requests that this Court:

A. Order this Complaint be filed without cost bond as provided by Tenn. Code Ann. §§ 47-18-108(b)(4) and 47-18-116;

B. Find that Defendants have violated Tenn. Code Ann. § 47-18-104(a), (b), and -2110 by engaging in the unlawful acts and practices herein;

C. Enter judgment against Defendants and in favor of the State for each violation alleged in this Complaint;

D. Enter a permanent injunction to prevent future violations of the TCPA by Defendants, pursuant to Tenn. Code Ann § 47-18-108(a)(5) and -2106;

E. Order Defendants to pay up to $1,000.00 per deceptive act or unfair practice that violates the TCPA, as provided in Tenn. Code Ann. § 47-18-108(b)(3);

F. Enter judgment against Defendants and in favor of the State for the reasonable costs and expenses of the investigation and prosecution of Defendants' actions, including attorneys' fees, expert and other witness fees, and costs, as provided by Tenn. Code Ann. § 47-18-108(a)(6) and (b)(4)

G. Order that all costs in this case be taxed against Defendants and no costs be taxed to the State as provided in Tenn. Code Ann. § 47-18-116; and

H. Award the State such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

HERBERT H. SLATERY III, B.P.R. No. 9077
Attorney General and Reporter

ANN MIKKELSEN, B.P.R. No. 032262
Assistant Attorney General
CAROLYN SMITH, B.P.R. No. 017166
Deputy Attorney General
Office of the Attorney General
Consumer Protection Division
UBS Building, 20th Floor
315 Deaderick Street
Nashville, Tennessee 37243
Phone: (615) 532-3819
Fax: (615) 532-2910
ann.mikkelsen@ag.tn.gov
carolyn.smith@ag.tn.gov

Attorneys for Plaintiff, State of Tennessee

IN THE CHANCERY COURT OF DAVIDSON COUNTY, TENNESSEE
FOR THE TWENTIETH JUDICIAL DISTRICT AT NASHVILLE

STATE OF TENNESSEE, *ex rel.* HERBERT H. SLATERY III, Attorney General and Reporter, Plaintiff, v. CHS/COMMUNITY HEALTH SYSTEMS INC., a Delaware corporation, and CHSPSC, LLC, f/k/a COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, a Delaware corporation, Defendants.	)	Case No. 20-1006-I

AGREED FINAL JUDGMENT

Plaintiff, the State of Tennessee, by and through Herbert H. Slatery III, Attorney General and Reporter for the State of Tennessee, and CHS/Community Health Systems, Inc. and CHSPSC, LLC, formerly Community Health Systems Professional Services Corporation, have agreed to the stipulations and terms of this Agreed Final Judgment (Agreed Judgment) without admission of any facts or liability of any kind as alleged in Plaintiff's civil enforcement action.

A. PARTIES

1. Plaintiff is the State of Tennessee, represented by Herbert H. Slatery III, Attorney General and Reporter for the State of Tennessee (Attorney General). The Attorney General is authorized to enforce the Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-101 to -131, the Tennessee Identity Theft Deterrence Act, Tenn. Code Ann. §§ 47-18-2101 to -2111, and the Health Insurance Portability and Accountability Act as amended by the Health Information

Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226, 42 U.S.C. § 1320d-5(d) (HIPAA).

2. Defendant CHS/Community Health Systems, Inc. (CHS/CHSI) is a Delaware corporation with its principal place of business at 4000 Meridian Blvd., Franklin, TN 37067-6325. It is the parent company of CHSPSC, LLC, and is a party to this Agreed Judgment by virtue of being a guarantor of CHSPSC's obligations herein.

3. Defendant CHSPSC, LLC, (CHSPSC) is a Delaware limited liability company that provides management and professional services to various hospitals and other healthcare providers affiliated with CHS/CHSI. CHSPSC employs the individuals and owns and controls the computer systems at issue in this Agreed Judgment. Its principal place of business is 4000 Meridian Blvd., Franklin, TN 37067.

B. BACKGROUND

4. The Attorneys General of the States and Commonwealths of Alaska, Arkansas, Connecticut, Florida, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Washington, and West Virginia (collectively, the "Attorneys General," or the "States") conducted an investigation of the data breach which Defendants disclosed in August 2014 (the Data Breach) pursuant to the authority of their respective State Consumer Protection Acts and/or where applicable, Personal Information Protection Acts and their authority under the Health Insurance Portability and Accountability Act as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226, 42 U.S.C. § 1320d-5(d) (HIPAA). Defendants are entering into an Agreed Judgment with each of the States and each State's

judgment incorporates the substantive terms included herein. To the extent there are differences, those differences are related to and/or arise from the requirements of local rules and state laws.

C. STIPULATIONS

5. Plaintiff and Defendants agree to and do not contest the entry of this judgment.

6. At all times relevant to this matter, Defendant CHSPSC engaged in trade and commerce affecting consumers in the States.

7. Defendant CHSPSC is a Business Associate and therefore is subject to the requirements of HIPAA and its Rules. CHSPSC is also subject to the States' consumer protection laws and may also be subject to certain state Personal Information Protection laws (*see* Appendix A).

8. Defendant CHS/CHSI consents to jurisdiction and venue only for purposes of entry of this Agreed Judgment as well as for the purpose of any subsequent action to enforce it. It does not consent to jurisdiction for any other purpose.

D. JURISDICTION

9. The Court finds it has jurisdiction over CHS/CHSI for purposes of entry of this Agreed Judgment as well as for the purpose of any subsequent action to enforce it.

10. The Court finds that it has jurisdiction over the subject matter and over the Parties for the purpose of entering and enforcing this Judgment. Further, the Court retains jurisdiction for the purpose of enabling the Parties to later apply to the Court for such further orders and relief as may be necessary for the construction, enforcement, execution or satisfaction of this Judgment.

E. DEFINITIONS

11. "Consumer Protection Acts" refers to the relevant state laws of the Participating States as cited in Appendix A.

12. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103 and refers to a person or entity that provides certain services for or performs functions on behalf of "Covered Entities," and requires access to Protected Health Information to provide such services or perform such functions.

13. "Covered Entity" or "Covered Entities" shall be defined in accordance with 45 C.F.R. § 160.103 and is a health care clearinghouse, health plan, or health care provider that transmits health information in electronic form in connection with a transaction for which the United States Department of Health and Human Services has adopted standards.

14. "Effective Date" shall be October 23, 2020.

15. "Encrypt" or "Encryption" shall mean to render unreadable, indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally in the field of information security

16. "HIPAA Privacy Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' medical records and other Protected Health Information as defined at 45 C.F.R. Parts 160 and subparts A and E of Part 164.

17. "HIPAA Security Rule" shall refer to the HIPAA regulations that establish national standards to safeguard individuals' Electronic Protected Health Information as defined at 45 C.F.R. Parts 160 and subparts A and C of Part 164.

18. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule as defined in 45 C.F.R. §§ 164.502(b) and 164.514(d).

19. "Personal Information" or "PI" shall have the same definition as "Personal Identifying Information" as set forth in the Personal Information Protection Acts of the Participating States.[1]

20. "Protected Health Information" or "PHI" is defined in accordance with 45 C.F.R. § 160.103.

21. "Personal Information Protection Acts" refers to the state laws of the Participating States as cited in Appendix B.

22. "Security Event" refers to any compromise, or threat that gives rise to a reasonable likelihood of compromise, by unauthorized access or inadvertent disclosure impacting the confidentiality, integrity, or availability of Personal Information or Protected Health Information of at least 500 United States consumers held or stored within Defendants' computer network, including but not limited to a Breach as defined in HIPAA at 45 CFR § 164.402 or the States' Personal Information Protection Acts. For purposes of this definition, "availability" shall not include an intentional limitation on the availability of Personal Information or Protected Health Information, such as for purposes of performing maintenance on Defendants' computer network, nor shall "availability" include circumstances where the information is available from other sources, including backup media.

23. "States" or "Participating States" refers to the following: Alaska, Arkansas, Connecticut, Florida, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Washington, and West Virginia.

[1] For Tennessee's purposes, "personal identifying information" means "personal information" as defined in the Tennessee Identity Theft Deterrence Act, Tenn. Code. Ann. § 47-18-2107.

24. "Third-Party Assessor" refers to an individual qualified as a Certified Information Systems Auditor or as a Certified Information Systems Security Professional who has at least five (5) years of experience evaluating the effectiveness of information system security or computer networks of Covered Entities.

F. INJUNCTIVE RELIEF

Now therefore, on the basis of these findings and stipulations, the relief in paragraphs 25 through 45 below is ordered:

Compliance with State and Federal Laws

25. Defendant CHSPSC shall comply with the Consumer Protection Acts, the Personal Information Protection Acts, and the HIPAA Privacy and Security Rules, to the extent they each are applicable to the Defendant, in connection with their collection, maintenance, and safeguarding of Personal Information and Protected Health Information from any future breach of security involving the unauthorized disclosure of PI or PHI.

Information Security Program

26. Defendant CHSPSC shall develop, implement, and maintain a written information security program ("Information Security Program" or "Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that they collect, store, transmit, and/or maintain. At a minimum, the Program shall include the information security requirements in (a) through (f) below.

a. The Program must be documented, in writing, and must contain administrative, technical, and physical safeguards appropriate to (i) the size and complexity of Defendants' and Defendants' affiliates' operations; (ii) the nature and scope of Defendants' and Defendants' affiliates' activities;

and (iii) the sensitivity of the PI and PHI that Defendant CHSPSC collects, stores, transmits, and/or maintains.

b. The Program shall permit users access to PI and PHI only to the extent necessary for each user to perform job functions and assignments.

c. Defendant CHSPSC shall employ an executive or officer whose full-time responsibility will be to implement, maintain, and monitor the Program (hereinafter referred to as the Chief Information Security Officer or CISO). The CISO shall have appropriate training, expertise, and experience in the field of information security appropriate to oversee the Program and further, will be charged with regular and direct reporting to the Board of Directors and Chief Financial Officer of Community Health Systems, Inc. regarding the status of the Program, the security risks faced by Defendant and Defendant's affiliates, resources required for implementation of the Program, and the security implications of Defendant's business decisions. At a minimum, the CISO shall provide a report to the Board on an annual basis and to the Chief Financial Officer on a quarterly basis.

d. Within 110 days of the Effective date, Defendant CHSPSC shall, as part of the Program, develop a documented written incident response plan to prepare for and respond to any future Security Events. At a minimum, this plan shall provide for the following phases of a response: Preparation; Detection and Analysis; Containment; Notification and Coordination with Law Enforcement and Regulators; Recovery; Consumer Notification and Remediation; and Post-Incident Analysis.

e. Defendant CHSPSC shall, as part of the Program, develop a patch management policy to address requirements for the application of security updates or security patches in a reasonable fashion and time frame, taking into account the severity of any vulnerability for which the update or patch has been released to address and the severity of the issue as reasonably determined by its CISO in the context of its overall network, any relevant compensating controls, and its ongoing business operations. The CISO's risk assessment should, at a minimum, include the identification of internal and external risks to the security that could result from the failure to timely apply security updates or patches, and an assessment of the safeguards in place to control these risks.

f. Defendant CHSPSC shall, as part of the Program, incorporate security awareness and privacy training for all personnel who have access to PI or PHI on proper compliance with Defendant's and its affiliates' approved policies and procedures. Training provided to personnel must be appropriate to job responsibilities and functions, and after the initial training, must be provided to personnel on at least an annual basis. Each employee who completes training shall certify, in writing or electronically, that he or she has completed the required training and include the date upon which such training was completed.

27. Defendants may satisfy the requirements to implement and maintain the Program, including the written incident response plan and the "Specific Information Security Requirements" noted below, through review, maintenance, and as necessary, updating of CHSPSC's existing

information security program and related safeguards, provided that such program and safeguards meet the requirements of this Agreed Judgment. Additionally, Defendants' agreement to undertake any obligations related to developing, fully implementing, and/or maintaining the Program is not intended as an admission of any liability or wrongdoing, or as evidence that either Defendants' existing information security program, including its written incident response plan, did not already meet or exceed the requirements of the Information Security Program and/or the Specific Information Security Requirements as set forth in this Agreed Judgment.

28. Defendant CHSPSC shall provide the resources and support necessary to fully implement the Program so that it functions as required and intended by this Agreed Judgment.

Specific Information Security Requirements

Policy of Minimum Necessary Access

29. Defendant CHSPSC shall collect and/or maintain PI and PHI only to the extent necessary to accomplish its intended purpose and to fulfill its regulatory, legal, and contractual obligations. In accordance with the Minimum Necessary Standard requirements of the Privacy Rule, Defendant shall limit unnecessary or inappropriate access to and disclosure of PI and PHI.

Access Controls

30. Defendant CHSPSC shall implement and maintain appropriate policies and controls to manage and limit access to, and use of, all accounts with access to PI or PHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Defendant's policies shall incorporate access rights based upon least privileged access that is granted only as absolutely necessary and required to perform routine, authorized activities.

Password Management

31. Defendant CHSPSC shall implement and maintain password policies and practices to manage access to, and use of, Defendant's and Defendant's affiliates' individual accounts, service accounts, and vendor accounts, including requiring strong and complex passwords and password rotation and prohibiting the use of default, group, shared or generic passwords. Further, passwords shall not be saved in plaintext.

Privileged Account Management

32. Defendant CHSPSC shall implement and maintain reasonable controls to secure the use of privileged credentials, such as through a Privileged Access Management tool, and shall require administrators to use multi-factor authentication or reasonably equivalent technology to gain access to credentials. Defendant shall also adopt a reasonable and risk-based approach requiring multi-factor authentication for remote access to Defendant's and Defendant's affiliates' networks that store, transmit, or permit access to PI or PHI.

Encryption

33. Defendant CHSPSC shall develop and maintain policies and procedures to encrypt PI and PHI at rest and in transit as reasonable and appropriate, and in accordance with applicable law. If Defendant CHSPSC uses File Transfer Protocol (FTP) to transmit PHI, it must utilize a secure and HIPAA-compliant FTP server for such activity. Provided, however, that any decision to transmit or store unencrypted PI or PHI shall be approved by the CISO, who shall conduct an appropriate risk assessment. Such a risk assessment shall include, at a minimum:

a. The identification of internal and external risks to the security, confidentiality, or integrity of PI and PHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other

compromise of such information if it is transmitted or stored without being encrypted;

b. An assessment of the safeguards in place to control these risks;

c. Documentation of any decision to transmit or store unencrypted PI or PHI and the approval of the CISO.

Annual Risk Assessment

34. Defendant CHSPSC shall obtain an annual risk assessment performed by a qualified outside third party and such assessment must at a minimum include:

a. The identification of internal and external risks to the security, confidentiality, or integrity of PI and PHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information;

b. An assessment of the safeguards in place to control these risks;

c. The evaluation and adjustment of the Program considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and

d. Documentation of safeguards implemented in response to such annual risk assessments.

Penetration Testing

35. Defendant CHSPSC shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities within its network. Such testing shall occur on at least a biannual basis and shall include penetration testing of Defendant's internal and external network defenses. Further, Defendant

CHSPSC shall review the results of these tests, take reasonable steps to remediate any critical findings revealed by such testing, and document their decision-making regarding such remediation.

Email Filtering and Phishing Solutions

36. Defendant CHSPSC shall implement and maintain email protection and filtering solutions, including protection against email SPAM and phishing attacks, for its employees, agents and affiliates.

Intrusion Detection and Data Loss Protection

37. Defendant CHSPSC shall implement and maintain an intrusion detection solution and data loss prevention technology to detect unauthorized access to its network and prevent unauthorized exfiltration of its data and must configure its systems to block FTP uploads or transmissions which contain PI or PHI.

Endpoint Detection

38. Defendant CHSPSC shall implement and maintain controls designed to provide real-time notification of anomalous activity and malicious system modifications within their network.

Logging

39. Defendant CHSPSC shall implement and maintain an appropriate system to collect and maintain logs and monitor network activity, such as through the use of a security information and event management (SIEM) tool, and shall further ensure that such tools are properly configured, regularly updated, and maintained to ensure that Security Events are timely reviewed and that appropriate follow-up and remediation steps are taken with respect to any Security Event.

Defendant CHSPSC shall further ensure that logs are protected from unauthorized access, destruction, and/or deletion.

Whitelisting

40. Defendant CHSPSC shall implement and maintain controls designed to block and/or prevent the execution of unauthorized applications on its network and to identify those applications which are permitted (whitelisted) within its network, to the extent such application whitelisting is reasonable and feasible pursuant to technical and/or financial limitations.

Business Associates

41. Defendant CHSPSC shall implement and maintain written policies and procedures related to Business Associates which at a minimum:

a. Designate one or more individual(s) who are responsible for ensuring that Defendant enters into a Business Associate agreement with each of its Business Associates, as defined by the HIPAA Rules, prior to disclosing PI or PHI to the Business Associate;

b. Assess Defendant's current and future business relationships to determine whether the relationship involves a Business Associate, as defined by the HIPAA Rules (this includes, but is not limited to, Defendant's agents and affiliates);

c. Implement and maintain a process for negotiating and entering into Business Associate agreements with Business Associates prior to disclosing PI or PHI to the Business Associates;

d. Implement and maintain risk-based policies and procedures for auditing Business Associate compliance with the terms of the Business Associate agreement;

e. Implement and maintain policies and procedures which limit disclosures of PI and PHI to the minimum amount that is reasonably necessary for Business Associates to perform their duties; and

f. Implement and maintain policies and procedures which retain documentation of a Business Associate agreement for at least six (6) years beyond the date that the Business Associate relationship is terminated.

Electronic Storage Media Policy

42. Defendant CHSPSC shall implement and maintain policies and procedures related to the use of hardware and electronic media that may be used to access, store, download, or transmit PI or PHI. Media may include, but are not limited to: servers, desktop computers, laptop computers, centrally managed storage media devices, tablets, mobile phones, USB drives, external hard drives, DVDs and CDs. This includes but is not limited to, employee personal devices and media able to obtain authorized access to Defendant's electronic ePHI systems (commonly referred to as "Bring Your Own Device").

Information Security Program Assessment

43. Within 120 days of the Effective Date and annually for 3 years thereafter, Defendant CHSPSC shall obtain an assessment of its Program pertaining to the collection, storage, maintenance, transmission, and disposal of PI and PHI from a Third-Party Assessor.

44. The Third-Party Assessor shall prepare a report of findings ("Report") and such report must include an assessment of Defendant's compliance with each of the requirements of

this Judgment; an assessment of Defendant's response to any Security Events which may have occurred since the Effective Date; and documentation of the basis of the Report.

45. Each report shall be provided to the Connecticut Attorney General no later than fifteen (15) days after its completion. Defendant may submit a separate letter with the Report documenting its responses to its findings. The Attorney General's office shall, to the extent permitted by state law, treat each report and letter (if submitted) as exempt from disclosure as applicable under the relevant public records laws of its state, provided that the Attorney General may provide a copy of each report and letter to any of the Participating States which request the report. Each participating State requesting the report shall, to the extent permitted by its State's law, treat such report and letter as exempt from disclosure as applicable under the relevant public records laws of the requesting State.

G. PAYMENT TO THE STATES

46. Within thirty (30) days of the Effective Date, Defendant CHSPSC shall pay Five Million Dollars to the Attorneys General, to be distributed to each Participating State as agreed by them. Tennessee's portion of the total amount shall be $ 666,686.77. The money received by the Attorneys General pursuant to this paragraph may be used by each Participating State for purposes that may include, but are not limited to, attorney's fees and other costs of investigation and litigation, or be placed in, or applied to, any consumer protection law enforcement fund, including consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund, or for such other uses permitted by state law, at the sole discretion of the state's Attorney General. If the Court has not entered this Judgment by its Effective Date, Defendants shall make the payment within twenty (20) days of the Effective Date or within fourteen (14) days of the entry of Judgment, whichever is later.

47. Following full payment of the amounts due by Defendant CHSPSC under this Judgment, the Attorney General shall release and discharge Defendants and their affiliates from any and all civil claims that the Attorney General could have brought that are related to and/or arising from the Data Breach, including but not limited to, any claims under the Consumer Protection Act, Personal Information Act, and HIPAA. Nothing contained in this paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that Defendants, their officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Judgment.

H. NOTICES

48. Unless otherwise provided, any notices or documents required to be sent to the Parties pursuant to this Judgment shall be sent to the following address via first class and electronic mail (unless after the Effective Date, a different address is communicated in writing by the party requesting the change of address):

For the Attorney General:

Deputy, Consumer Protection Division
Office of the Tennessee Attorney General
P.O. Box 20207
Nashville, Tennessee 37202-0207
Phone: (615) 741-1671

For Defendants:

Justin Pitt
Senior Vice President and Chief Litigation Counsel
CHSPSC, LLC
4000 Meridian Blvd.
Franklin, Tennessee 37064

I. GENERAL PROVISIONS

49. The terms of this Judgment are not intended to be construed as an admission or concession or evidence of liability or wrongdoing on the part of Defendants or their affiliates. More specifically, Defendants' agreement to undertake any obligations, including the obligations set forth in paragraphs 25 – 45 described in this Judgment, is not intended to be construed as an admission of liability or wrongdoing of any kind, nor as evidence that Defendants' existing information security program, including its written incident response plan, did not already meet or exceed the requirements of the Information Security Program and/or the Specific Information Security Requirements as set forth in this Judgment.

50. Acceptance and entry of this Judgment is not an approval of any of Defendants' advertising or business practices.

51. Defendants will not participate in any activity to form a separate entity for the purpose of engaging in acts or practices prohibited by this Judgment or for any other purpose that would circumvent this Judgment.

52. Nothing in this Judgment shall be construed to limit the authority of the State to protect the interests of the State or its citizens, or to enforce any laws, regulations, or rules against Defendants.

53. This Judgment does not affect any private right of action that any consumer, person, entity, or federal, state, or local governmental entity may have against Defendants.

54. Nothing in this Judgment waives or affects any claims of sovereign immunity by the State.

55. Defendants waive the notice provisions under Tenn. Code Ann. § 47-18-108(a)(2)

and waive any defect in connection with service of process. Defendants also waive compliance with Tenn. Code Ann. § 47-18-5002(2), in accordance with Tenn. Code Ann. § 47-18-108(a)(3).

56. Defendants expressly waive any rights, remedies, appeals, or other interests related to a jury trial or any related or derivative rights under the Tennessee or United States Constitutions or other laws as to this Judgment.

57. This Court must approve all modifications to this Judgment.

58. If any provision of this Judgment shall be held unenforceable, the Judgment shall be construed as if such provision did not exist.

59. This Judgment may be executed in counterparts that, together, will constitute one whole document.

60. Within 30 days of this Judgment's entry, Defendants shall provide a copy of this Judgment to each of their officers and directors, owners, employees, and applicable agents. Once provided, Defendants shall, within 45 days of this Judgment's entry, provide a certification under oath to the State that affirms compliance with this paragraph.

61. All costs associated with this action and Judgment shall be borne by Defendants, and no costs shall be taxed to the State.

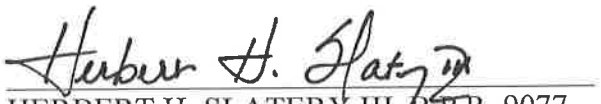
62. This Judgment sets forth the entire agreement between the Parties.

IT IS SO ORDERED.

_____

CHANCELLOR

JOINTLY APPROVED AND SUBMITTED FOR ENTRY:



HERBERT H. SLATERY III, B.P.R. 9077
Attorney General and Reporter of Tennessee

ANN MIKKELSEN, B.P.R. 032262
Assistant Attorney General
CAROLYN SMITH, B.P.R. 017166
Deputy Attorney General
Consumer Protection Division
P.O. Box 20207
Nashville, Tennessee 37202-0207
T: (615) 253-3819
F: (615) 532-2910
Email: ann.mikkelsen@ag.tn.gov
carolyn.smith@ag.tn.gov

ATTORNEYS FOR THE STATE OF TENNESSEE

JOINTLY APPROVED AND SUBMITTED FOR ENTRY:

DEFENDANT, CHS/Community Health Systems, Inc. (CHS/CHSI) and CHSPSC, LLC, formerly Community Health Systems Professional Services Corporation (CHSPSC)

By: _____ **Date:** 9-22-20

JUSTIN PITT
Senior Vice President and Chief Legal Counsel
CHSPSC, LLC

JOINTLY APPROVED AND SUBMITTED FOR ENTRY:

ATTORNEYS FOR DEFENDANTS:
CHS/Community Health Systems, Inc. (CHS/CHSI) and CHSPSC, LLC, formerly Community Health Systems Professional Services Corporation (CHSPSC)

By: Eric A Packel **Date:** 9/23/2020

Theodore J. Kobus, III
Baker & Hostetler, LLP
45 Rockefeller Plaza, 14th Floor
New York, NY 10111
Tel: (212) 589-4200
Fax: (212) 589-4201

Eric A. Packel
Baker & Hostetler, LLP
Cira Centre, 12th Floor
2929 Arch Street
Philadelphia, PA 19104
Tel: 215-564-3031
Fax: 215-566-3439

JOINTLY APPROVED AND SUBMITTED FOR ENTRY:

ATTORNEYS FOR DEFENDANTS:
CHS/Community Health Systems, Inc. (CHS/CHSI) and CHSPSC, LLC, formerly Community Health Systems Professional Services Corporation (CHSPSC)

By:  **Date:** 09/23/2020

Donald B. Hutchins (#033364)
Baker & Hostetler, LLP
1801 California Street, Suite 4400
Denver, CO 80202
Telephone: (303) 764-4071
Facsimile: (303) 861-7805
dhutchins@bakerlaw.com

Appendix A.

STATE	UDAP/DTPA AUTHORITY
Alaska	Unfair Trade Practices Act, AS 45.50.471 *et seq.*
Arkansas	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101, *et seq.*
Connecticut	Connecticut's Unfair Trade Practices Act ("CUTPA"), General Statutes § 42-110b *et seq.*
Florida	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes (2019)
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*
Indiana	Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 ("DCSA")
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Kentucky	Kentucky Consumer Protection Act, KRS 367.110 to .300 and KRS 367.990
Louisiana	Unfair Trade Practices and Consumer Protection Law, La. R.S. 51:1401 *et seq.*
Massachusetts	Massachusetts Consumer Protection Act, G.L. c. 93A
Michigan	Michigan Consumer Protection Act, MCL 445.901, *et seq.*
Mississippi	Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1 *et seq.;*
Missouri	Missouri Merchandising Practices Act, Chapter 407, RSMo
Nebraska	Consumer Protection Act, Neb. Rev. Stat. § 59-1601 *et seq.*; Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.*
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903, *et seq.*
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -226.
North Carolina	North Carolina Unfair and Deceptive Trade Practices Act, N.C. G. S. §§ 75-1.1, *et seq.*
Ohio	Ohio Consumer Sales Practices Act, R.C. 1345.01 *et seq.*

Appendix A.

Oregon	Oregon Unlawful Trade Practices Act, ORS 646.605 *et seq.*
Pennsylvania	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 *et seq.*
Rhode Island	Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1, *et seq.*
South Carolina	South Carolina Unfair Trade Practices Act §§39-5-10 *et seq. (SCUTPA)*
Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -131
Texas	Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann.§§ 17.41-17.63
Utah	Utah Consumer Sales Practices Act, Utah Code §§ 13-11-1, *et. seq.*
Vermont	Vermont Consumer Protection Act, 9 V.S.A. § 2453
Washington	Washington Consumer Protection Act, RCW § 19.86.020
West Virginia	West Virginia Consumer Credit and Protection Act ("WVCCPA"), W. Va. Code §§ 46A-1-101 *et seq.*, [W. Va. Code § 46A-6-104 § 46A-6-102(7)(G), and § 46A-6-102(7)(M)]

Appendix B.

STATE	
Alaska	Personal Information Protection Act, AS 45.48.010 *et seq.*
Arkansas	Personal Information Protection Act, Ark. Code Ann. § 4-110-101, *et seq.*
Connecticut	Connecticut's Data Breach Notification Law, General Statutes § 36a-701b; and the Safeguards Law, General Statutes § 42-471
Florida	Florida Information Protection Act, Section 501.171, Florida Statutes (2019)
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*
Indiana	Disclosure of Security Breach Act, Ind. Code § 24-4.9 ("DSBA")
Iowa	Personal Information Security Breach Protection Act, Iowa Code Ch. 715C
Kentucky	Records Containing Personally Identifiable Information, KRS 365.7342 *et seq.*
Louisiana	Database Security Breach Notification Law, La. R.S. 51:3071 *et seq.*
Massachusetts	Massachusetts Data Security Law, G.L. c. 93H
Mississippi	Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-29
Nebraska	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.*
Nevada	Nevada Security of Personal Information Act; Nev. Rev. Stat. §§ 603A.010 – 603A.290
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -226.
North Carolina	North Carolina Identity Theft Protection Act, N.C. G. S. §§ 75-60, *et seq.*
Ohio	Ohio Private Disclosure of Security Breach of Computerized Personal Information Data, R.C. 1349.19
Oregon	Oregon Consumer Information Protection Act, ORS 646A.600 *et seq.*

Appendix B.

Rhode Island	Rhode Island Identity Theft Protection Act of 2015 R.I. Gen. Laws § 11-49.3-1, *et seq.*
South Carolina	Family and Personal Identifying Information Privacy Protection Act §§ 30-2-10 *et seq.*
Tennessee	Tennessee Identity Theft Deterrence Act of 1999, §§ 47-18-2101 to -2111
Texas	Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 -152
Utah	Utah Protection of Personal Information Act, Utah Code §§ 13-44-101, *et. seq.*
Vermont	Vermont Consumer Protection Act, 9 V.S.A. § 2453
Washington	Washington Data Breach Notification Law, RCW §§ 19.225.005, *et seq.*
West Virginia	West Virginia Consumer Credit and Protection Act ("WVCCPA"), W.Va. Code §§ 46A-1-101 *et seq.*, more specifically W. Va. Code § 46A-2A-10 *et seq.*