



Advanced Reading Materials for
The Evolving Enforcement and Litigation Landscape for Health Data
May 9, 2024 4-5 PM

- I. Links to Selection of FTC Cases, Rules, and Guidance Related to Privacy of Health Information
 - Health Breach Notification Rule
 - Health Privacy
 - Biometric & Genetic Information

- II. Complaints and Consent Judgments from Selection of State Attorney General Actions
 - *State of Indiana v. Carepointe, P.C.*
 - *State of Indiana v. Jackson County Schneck Memorial Hospital*
 - *State of Indiana v. DXC Technology Services, LLC*

Health Privacy Information

Health Breach Notification Rule

Federal Register Announcing Final Rule

<https://www.ftc.gov/legal-library/browse/federal-register-notice/health-breach-notification-final-rule>

Business Guidance

Updated Health Breach Notification Rule puts new provisions in place to protect users of health apps and devices

https://www.ftc.gov/business-guidance/blog/2024/04/updated-ftc-health-breach-notification-rule-puts-new-provisions-place-protect-users-health-apps?utm_source=govdelivery

Mobile Health App Interactive Tool

<https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool>

Health Privacy

FTC and HHS Warning Letter to Hospital Systems and Other Telehealth Providers

<https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>

Business Guidance

The DNA of privacy and the privacy of DNA

<https://www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna>

Blog: Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking

<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>

Blog: Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal sharing of highly sensitive data

<https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>

Blog: Protecting the privacy of health information: A baker's dozen of takeaways from FTC cases

<https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>

Collecting, Using, or Sharing Consumer Health Information: Look to HIPAA, the FTC Act, and the Health Breach Notification Rule

<https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach>

Recent Cases

Monument: https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentComplaintFiled.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf

Cerebral: https://www.ftc.gov/system/files/ftc_gov/pdf/2223087cerebralcomplaint.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/cerebral_joint_stipulation_order_permanent_injunction.pdf

BetterHelp: https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpcomplaintfinal.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf

GoodRx: https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf

Premom: https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf

Vitagene: https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-Complaint.pdf
https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-DecisionandOrder.pdf

FloHealth: https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf
https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf

Biometric & Genetic Information

Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the FTC Act

https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf

Blog: Selling genetic testing kits? Read on.

<https://www.ftc.gov/business-guidance/blog/2019/03/selling-genetic-testing-kits-read>

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

CAREPOINTE, P.C.,

Defendant.

Case No. 2:23-cv-328

**COMPLAINT FOR INJUNCTIVE
RELIEF, DAMAGES, ATTORNEY
FEES AND COSTS**

REQUEST FOR JURY TRIAL

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by Deputy Attorney General Jennifer M. Van Dame, brings this action for injunctive relief, statutory damages, attorney fees, and costs against CarePointe, P.C. (“CarePointe”) for violations of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”), stemming from CarePointe’s deficient security practices contributing to a data breach affecting over 45,000 patients and CarePointe’s misrepresentations to patients regarding its security practices. In support of its Complaint, the State alleges:

I. PARTIES, JURISDICTION, AND VENUE

1. The Indiana Attorney General is authorized to bring this action to enforce HIPAA pursuant to 42 U.S.C. § 1320d-5(d). The Indiana Attorney General is authorized to bring this action to enforce the DSBA pursuant to Ind. Code § 24-4.9-4-2, and the DCSA pursuant to Ind. Code § 24-5-0.5-4(c).

2. CarePointe, P.C. (“CarePointe”) is an Indiana professional corporation with a principal office located at 99 E 86th Ave, Suite A, Merrillville, IN 46410.

3. This Court has jurisdiction pursuant to 42 U.S.C. § 1320d-5(d)(1) and 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C § 1367.

4. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2).

5. The State has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. §1320d-5(d)(4).

II. FACTUAL ALLEGATIONS

6. At all times relevant to this Complaint, CarePointe provided health care services to Indiana residents and was a covered entity within the meaning of HIPAA. *See* 45 C.F.R. § 160.103.

7. On or around June 25, 2021, sensitive patient information was exfiltrated from CarePointe’s systems during a ransomware event (the “Data Breach”).

8. CarePointe provided notification of the Data Breach to patients and the

State on August 23, 2021.

9. The Data Breach exposed the personal information and/or protected health information (“PHI”) of approximately 45,002 Indiana residents.

10. The categories of personal information and/or PHI exposed by the Data Breach included: names, addresses, dates of birth, Social Security numbers, medical insurance information, and health information.

11. CarePointe’s Notice of Privacy Practices (effective March 24, 2003),¹ touts “OUR COMMITMENT TO PROTECTING HEALTH INFORMATION ABOUT YOU”, stating:

- a. “We consider it our great privilege to serve your medical needs and we value the trust you have placed in us. We are committed to safeguarding your patient information . . .”;
- b. “The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient . . .”; and
- c. “We are required by law to: Maintain the privacy of PHI about you . . .”

12. Moreover, CarePointe’s Notice of Privacy Practices Acknowledgement,²

¹ Notice of Privacy Practices, CarePointe Ear, Nose, Throat and Sinus Centers, *available at* https://carepointe.net/wp-content/uploads/2016/05/Notice_of_Privacy_Practices.pdf (last accessed Sept. 22, 2023).

² Notice of Privacy Practices Acknowledgement, *available at* https://carepointe.net/wp-content/uploads/2016/07/Notice_of_Privacy_Practices-Acknowledgement.pdf (last accessed Sept. 22, 2023).

requires patients to acknowledge that they have “received, read and understand” CarePointe’s Notice of Privacy Practices and certify: “I understand that, under the Health Insurance Portability & Accountability Act of 1996 (“HIPAA”), I have certain rights to privacy regarding my protected health information.”

13. Notwithstanding CarePointe’s representations regarding its commitment to patient privacy in its Notice of Privacy Practices and Notice of Privacy Practices Acknowledgement, CarePointe lacked appropriate security policies, failed to conduct appropriate risk assessments, and failed to promptly address known security issues.

14. In or around late 2020, CarePointe had initial meetings with an IT vendor who flagged CarePointe’s remote access policies as a security issue that needed to be addressed (the “IT Vendor”).

15. By January 2021, the IT Vendor completed a written HIPAA risk assessment that put CarePointe on notice of many additional security issues that contributed to the Data Breach later that year, including:

- a. Weak password policies, including no password expiration, passwords of less than 8 characters allowed, and no password complexity requirement;
- b. Account lockout after a number of failed login attempts disabled;
- c. Active Directory contained inactive/decommissioned computers;
- d. A number of users not logged in for an extended period indicating a lack of procedures for terminating user access;

- e. Outdated anti-virus software;
- f. Unrestricted access rights to network shares containing PHI; and
- g. Use of generic logins for systems containing PHI.

16. CarePointe eventually hired the IT Vendor in March 2021 to address the security issues flagged in the January 2021 HIPAA risk assessment, but the work was not completed before the Data Breach in June 2021.

17. CarePointe did not move quickly enough to address the significant risks that had developed after years of poor security practices.

18. The threat actor who deployed ransomware on CarePointe's systems gained access from outside of CarePointe's network via an open, unsecured port used for remote access.

19. The security issues flagged by the IT Vendor allowed the threat actor to infiltrate CarePointe's network undetected, exfiltrate patient data, and execute ransomware to fully encrypt all systems.

20. If CarePointe had maintained appropriate security policies, conducted appropriate risk assessments, and implemented a risk management plan to mitigate the risks identified by the risk assessments, as required by HIPAA, the obvious and significant security issues flagged by the IT Vendor in late 2020 and early 2021 would have been identified and addressed sooner.

21. CarePointe also failed to execute a business associate agreement with the IT Vendor until April 29, 2021, *after* the IT Vendor received access to CarePointe's systems to complete the January 2021 HIPAA risk assessment.

22. The IT Vendor also flagged the use of public domain email accounts such as MSN for CarePointe business, which continued through April 2022.

III. HIPAA BACKGROUND

23. As a covered entity, CarePointe was required to comply with the HIPAA standards that govern the privacy and security of PHI. *See* 45 C.F.R. Part 164.

24. The HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) requires covered entities to ensure the confidentiality, integrity, and availability of all PHI that the covered entity creates, receives, maintains, or transmits and to protect against any reasonably anticipated threats to the security or integrity of such information. *See* 45 C.F.R. § 164.306. To this end, the HIPAA Security Rule requires covered entities to employ appropriate administrative, physical, and technical safeguards to maintain the security and integrity of PHI. *See* 45 C.F.R. §§ 164.308, 164.310, 164.312.

25. It is the covered entity's responsibility to ensure compliance with HIPAA, including the Security Rule. A covered entity may delegate its obligations under the Security Rule to a business associate, such as an IT vendor, but the covered entity is liable for an agent's failure to comply with the Security Rule. *See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act*, 78 FR 5580-5581 (Jan. 25, 2013).

26. Finally, the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) prohibits covered entities from using or disclosing PHI, except as permitted by HIPAA.

IV. CAUSES OF ACTION

COUNT ONE: FAILURE TO COMPLY WITH HIPAA SECURITY RULE

27. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

28. The State investigated CarePointe's compliance with the Security Rule after CarePointe notified the State of the Data Breach.

29. Leading up to the Data Breach, CarePointe failed to employ appropriate safeguards to maintain the security and integrity of PHI, including as follows:

- a. CarePointe failed to implement, review, and/or modify policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §§ 164.308(a)(1)(i) and 164.306(e);
- b. CarePointe failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- c. CarePointe failed to implement procedures for terminating access to PHI when the employment of, or other arrangement with, a workforce member ends or as required, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(3)(C);
- d. CarePointe failed to implement procedures for guarding against, detecting, and reporting malicious software, or reasonable and

appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(B);

- e. CarePointe failed to implement procedures for monitoring log-ins, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(C);
- f. CarePointe failed to implement procedures for creating, changing, and safeguarding passwords, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);
- g. CarePointe failed to implement technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. CarePointe failed to assign unique names and/or numbers for identifying and tracking user identity in violation of 45 C.F.R. § 164.312(a)(2)(i);
- i. CarePointe failed to implement a mechanism to encrypt PHI at rest, or reasonable and appropriate alternatives to such mechanisms with documentation in violation of 45 C.F.R. § 164.312(a)(2)(iv);
- j. CarePointe failed to implement procedures to verify that a person seeking access to PHI is the one claimed in violation of 45 C.F.R. § 164.312(d).

- k. Prior to January 2021, CarePointe failed to conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by CarePointe in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);
 - l. Prior to January 2021, CarePointe failed to implement a risk management plan that applies security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B); and
 - m. CarePointe failed to execute an appropriate business associate agreement with its IT Vendor until *after* the IT Vendor received access to CarePointe's systems to complete a HIPAA risk assessment in violation of 45 C.F.R. § 164.308(b).
30. Each security issue identified in Paragraph 29, Subparagraphs (a)-(m) is a separate, continuing violation of the Security Rule that arose before the Data Breach.
31. For continuing violations, 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406 authorize statutory damages of \$100 per HIPAA violation, per day, totaling up to \$25,000 per year for violations of an identical requirement or prohibition.

**COUNT TWO:
FAILURE TO COMPLY WITH HIPAA PRIVACY RULE**

32. The State incorporates by reference all preceding paragraphs as if fully set forth herein.
33. As a covered entity, CarePointe was prohibited from disclosing PHI

except as permitted by HIPAA. 45 C.F.R. § 164.502(a).

34. HIPAA defines “disclosure” as “the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.” 45 C.F.R. § 160.103.

35. CarePointe’s deficient security practices subjected the PHI of approximately 45,002 Indiana residents to disclosure during the Data Breach.

36. The disclosures were not permitted under any HIPAA exception.

37. Each disclosure was a separate violation of the Privacy Rule.

38. 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406 authorize statutory damages of \$100 per HIPAA violation, totaling up to \$25,000 per year.

**COUNT THREE:
FAILURE TO IMPLEMENT AND MAINTAIN
REASONABLE PROCEDURES IN VIOLATION OF
INDIANA DISCLOSURE OF SECURITY BREACH ACT**

39. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

40. The DSBA requires a data base owner to “implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.” Ind. Code § 24-4.9-3-3.5(c).

41. The DSBA defines “personal information” to include:

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual’s first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

- (A) A driver's license number.
- (B) A state identification card number.
- (C) A credit card number.
- (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Ind. Code § 24-4.9-2-10.

42. The categories of personal information exposed by the Data Breach included names and Social Security numbers.

43. CarePointe violated the DSBA by failing to implement and maintain reasonable security procedures to protect and safeguard personal information of Indiana residents.

44. CarePointe is not exempt from the DSBA because CarePointe was not in compliance with HIPAA at the times relevant to this Complaint. *See* Ind. Code § 24-4.9-3-3.5(a).

**COUNT FOUR:
VIOLATIONS OF INDIANA DECEPTIVE CONSUMER SALES ACT**

45. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

46. The DCSA regulates unfair, abusive, and/or deceptive acts, omissions, and/or practices between suppliers and consumers engaging in consumer transactions. *See* Ind. Code § 24-5-0.5-3.

47. Under the DCSA, a "consumer transaction" includes services and other intangibles. Ind. Code § 24-5-0.5-2(a)(1).

48. In supplying Indiana patients with health care services, CarePointe regularly engages in consumer transactions in Indiana and is a "supplier" as defined

by Ind. Code § 24-5-0.5-2(a)(3).

49. The DCSA prohibits a supplier from committing “an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.” Ind. Code. § 24-5-0.5-3(a).

50. It is a deceptive act under the DCSA to represent to consumers that the subject of a consumer transaction “has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have,” or “is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.” Ind. Code § 24-5-0.5-3(b)(1)-(2).

51. In its Notice of Privacy Practices, CarePointe represented to patients that it is committed to “PROTECTING HEALTH INFORMATION ABOUT YOU”, stating: “We consider it our great privilege to serve your medical needs and we value the trust you have placed in us. We are committed to safeguarding your patient information . . .”

52. CarePointe also implicitly represented that it is compliant with HIPAA and other applicable laws by:

- a. Stating its Notice of Privacy Practices: “The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient . . .”; and “We are required by law to:

Maintain the privacy of PHI about you . . . ”; and

- b. Requiring patients to certify in its Notice of Privacy Practices Acknowledgement: “I understand that, under the Health Insurance Portability & Accountability Act of 1996 (“HIPAA”), I have certain rights to privacy regarding my protected health information.”

53. Contrary to these representations, CarePointe knowingly failed to implement and maintain reasonable security practices to protect patients’ PHI.

54. CarePointe also knowingly failed to comply with HIPAA by failing to promptly address the security issues flagged by its IT Vendor in late 2020 and early 2021.

55. CarePointe explicitly and implicitly misrepresented that its systems were secure and compliant, when CarePointe knew they were not.

56. CarePointe knowingly committed unfair, abusive, and/or deceptive acts, omissions, and/or practices in connection with consumer transactions in violation of the DCSA, subjecting it to a civil penalty of up to \$5,000 per violation under Ind. Code § 24-5-0.5-4(g).

V. PRAYER FOR RELIEF

WHEREFORE, the State of Indiana respectfully requests that this Court enter judgment against CarePointe and in favor of the State as follows:

- a. Finding that CarePointe violated HIPAA, DSBA, and DCSA by engaging in the unlawful acts and practices alleged herein, and permanently enjoining

CarePointe from continuing to engage in such unlawful acts and practices pursuant to 42 U.S.C. § 1320d-5(d)(1)(A), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c);

b. Ordering CarePointe to pay statutory damages of \$100 per HIPAA violation, per day, totaling up \$25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406;

c. Ordering CarePointe to pay a \$5,000 civil penalty for violating the DSBA, as provided by Ind. Code § 24-4.9-3-3.5(f);

d. Ordering CarePointe to pay a \$5,000 civil penalty for each knowing violation of the DCSA alleged herein, as provided by Ind. Code § 24-5-0.5-4(g);

e. Ordering CarePointe to pay all costs and fees for the investigation and prosecution of this action pursuant to 42 U.S.C. § 1320d-5(d)(3), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c); and

f. Granting any such further relief as the Court may deem appropriate.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all issues so triable.

Respectfully submitted,

STATE OF INDIANA EX REL.
INDIANA ATTORNEY GENERAL
TODD ROKITA

Date: September 29, 2023

/s/ Jennifer M. Van Dame

Jennifer M. Van Dame
Indiana Attorney No. 32788-53
Deputy Attorney General
Data Privacy & Identity Theft Unit
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037
Phone: 317-232-0486
Fax: 317-232-7979
Email: jennifer.vandame@atg.in.gov

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION**

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

CAREPOINTE, P.C.,

Defendant.

Case No. 2:23-cv-328-PPS-JPK

CONSENT JUDGMENT AND ORDER

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by counsel, Deputy Attorney General Jennifer M. Van Dame, and Defendant, CarePointe, P.C. (“CarePointe”) (collectively, the “Parties”), have agreed to the Court’s entry of this Consent Judgment and Order (“Consent Judgment”) without trial or adjudication of any issue of fact or law.

This Consent Judgment resolves the Plaintiff’s investigation of the data breach described in the Complaint filed in this action regarding CarePointe’s compliance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and

Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”) (collectively, the “Relevant Laws”).

This Consent Judgment is not intended and shall not be used or construed as an admission by Defendant of any violation of the Relevant Laws, nor shall it be construed as an abandonment by the State of its allegations that Defendant violated the Relevant Laws.

The Parties consent to entry of this Consent Judgment by the Court as a final determination and resolution of the issues alleged in the Complaint.

THE PARTIES

1. The Office of the Indiana Attorney General (“OAG”) is charged with enforcement of the Relevant Laws, including HIPAA pursuant to 42 U.S.C. § 1320d-5(d).

2. CarePointe, P.C. (“CarePointe”) is an Indiana Professional Corporation with a principal office located at 99 E 86th Ave, Suite A, Merrillville, IN 46410.

BACKGROUND

3. On or around June 25, 2021, CarePointe was the target of a ransomware attack that exposed the Personal Information and/or Protected Health Information of approximately 45,002 Indiana residents.

4. The OAG investigated this incident pursuant to the Relevant Laws.

STIPULATIONS

5. The Parties agree to and do not contest the entry of this Consent Judgment.

6. At all times relevant to this matter, CarePointe was engaged in trade and commerce affecting consumers in the State of Indiana insofar as CarePointe provided health care services to consumers in Indiana. CarePointe was also in possession of the Personal Information and Protected Health Information of Indiana residents.

7. At all times relevant to this matter, CarePointe was a Covered Entity subject to the requirements of HIPAA.

8. The Parties consent to jurisdiction and venue in this Court for purposes of entry of this Consent Judgment as well as for the purpose of any subsequent action to enforce it.

JURISDICTION

9. The Court finds that it has jurisdiction over the Parties for purposes of entry of this Consent 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 of this Consent Judgment pursuant to 42 U.S.C. § 1320d-5(d), 28 U.S.C. § 1331, and 28 U.S.C. § 1367 for the purpose of entering and enforcing the Consent Judgment, and venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1). 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 Consent Judgment.

ORDER

NOW THEREFORE, the Court has reviewed the terms of this Consent Judgment and based upon the Parties' agreement and for good cause shown, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED AS FOLLOWS:

DEFINITIONS

11. For the purposes of this Consent Judgment, the following definitions shall apply:

- a. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 and are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
- b. "Breach" shall be defined in accordance with 45 C.F.R. § 164.402 to mean "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."
- c. "Business Associate" shall be defined in accordance with 45 C.F.R. §

160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to Protected Health Information.

- d. “Covered Entity” 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 U.S. Department of Health and Human Services has adopted standards.
- e. “DCSA” means the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.*, and any related statutes and rules adopted pursuant thereto. The DCSA is incorporated fully herein including all terms and definitions set forth therein.
- f. “DSBA” means the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.*, and any related statutes and rules adopted pursuant thereto. The DSBA is incorporated fully herein including all terms and definitions set forth therein.
- g. “Effective Date” shall mean the date on which this Consent Judgment is approved by the Court.
- h. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- i. “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.

- j. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and any related Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* HIPAA is incorporated fully herein including all terms and definitions set forth therein.
- k. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).
- l. “Personal Information” or “PI” shall be defined in accordance with Ind. Code § 24-4.9-2-10.
- m. “Privacy Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ medical records and other

Protected Health Information, including ePHI, that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

- n. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- o. “Security Incident” shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.
- p. “Security Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ Electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.
- q. “Technical Safeguards” shall be defined in accordance with 45 C.F.R. § 164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

INJUNCTIVE PROVISIONS

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE

COMPLIANCE WITH THE LAW:

Compliance with Federal and State Laws

8. Defendant shall comply with the HIPAA Privacy and Security Rules and shall implement all Administrative and Technical Safeguards required by HIPAA.

9. Defendant shall comply with DSBA and DCSA in connection with its collection, maintenance, and safeguarding of PI, PHI, and ePHI.

10. Defendant shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which Defendant maintains and/or protects the privacy, security, confidentiality, or integrity of PI, PHI, or ePHI.

Information Security Program

11. Overview: Within one hundred and twenty (120) days after the Effective Date, Defendant shall develop, implement, and maintain a written information security program (“Information Security Program” or “WISP”) that shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendant’s operations; (ii) the nature and scope of Defendant’s activities; and (iii) the sensitivity of the information that Defendant maintains. At a minimum, the WISP shall include the Specific Technical Safeguards and Controls in Paragraphs 17 through 28 below. Defendant may satisfy the requirements to implement and maintain the WISP through review, maintenance, and as necessary, updating of an existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Consent

Judgment. Defendant shall provide the resources and support necessary to fully implement the WISP so that it functions as required and intended by this Consent Judgment.

12. Governance: Defendant shall designate an individual whose responsibility will be to implement, maintain, and monitor the WISP (hereinafter referred to as the “HIPAA Security Officer” or “HSO”). The HSO shall have appropriate training to oversee the WISP and shall regularly report to the executive management regarding the status of the WISP, the security risks faced by the Defendant, resources required for implementation of the WISP, and the security implications of Defendant’s business decisions. At a minimum, the HSO shall report to the executive management any future Security Incident within twenty-four (24) hours of discovery, and shall also provide a copy of the documented Security Incidents and their outcomes to the executive management as needed in accordance with 45 C.F.R. § 164.308(a)(6)(ii).

13. Incident Response Plan: Defendant shall implement and maintain a written incident response plan (“Plan”) to prepare for and respond to any future Breaches. Defendant shall review and update the Plan as necessary. At a minimum, the Plan shall provide for the following phases:

- a. Preparation;
- b. Detection and Analysis;
- c. Containment;
- d. Notification and Coordination with Law Enforcement;

- e. Eradication;
- f. Recovery;
- g. Consumer and Regulator Notification; and
- h. Post-Incident Analysis and Remediation.

14. Table-Top Exercises: Defendant shall conduct, at a minimum, appropriate incident response plan exercises, every 18 months, to test and assess its preparedness to respond to Security Incidents and Breaches.

15. Training: Within one hundred and twenty (120) days of the Effective Date, and at least annually thereafter, Defendant shall provide data security and privacy training to all personnel with access to PI, PHI, or ePHI. Defendant shall provide this training to any employees newly hired to, or transitioned into, a role with access to PI, PHI, or ePHI, within thirty (30) days of hire or transition. Such training shall be appropriate to employees' job responsibilities and functions. Defendant shall document the trainings and the date(s) upon which they were provided.

16. Business Associates: Defendant shall develop, implement, and maintain written policies and procedures related to Business Associates, which at a minimum:

- a. Designate an individual as responsible for ensuring that Defendant enters into a Business Associate agreement with each of its Business Associates, prior to disclosing PI, PHI, or ePHI to the Business Associates;
- b. Assess Defendant's current and future business relationships to determine whether the relationship involves a Business Associate;

- c. Ensure that Defendant is entering into Business Associate agreements with Business Associates prior to disclosing PI, PHI, or ePHI to the Business Associates; and
- d. Ensure that Defendant is limiting disclosures of PI, PHI, or ePHI to the minimum amount necessary for the Business Associate to perform their duties.

17. Minimum Necessary Standard: Defendant shall design and update the WISP consistent with the Minimum Necessary Standard.

Specific Technical Safeguards and Controls

18. Password Management: Defendant shall implement and maintain password policies and procedures requiring the use of strong, complex passwords with reasonable password-rotation requirements and ensuring that stored passwords are protected from unauthorized access.

19. Account Management: Defendant shall implement and maintain policies and procedures to manage, and limit access to and use of, all accounts with access to PI or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Defendant shall not permit use of shared accounts with access to PI or ePHI.

20. Access Controls: Defendant shall implement and maintain policies and procedures to ensure that access to PI and ePHI is granted under the principle of least privilege. Such policies and procedures shall further include a means to regularly review access and access levels of users and require removal of network and

remote access within three (3) business days of notification of termination for any employee or vendor whose relationship with CarePointe has ended.

21. Multi-Factor Authentication: Defendant shall require the use of appropriate multi-factor authentication for remote access to Defendant's systems.

22. Asset Inventory: Defendant shall regularly inventory and classify all assets that comprise Defendant's network. The asset inventory shall, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the network; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores PI or ePHI; and (g) each security update or patch applied or installed during the preceding period.

23. Vulnerability Scanning: Defendant shall conduct regular vulnerability scanning using industry-standard tool(s) and shall take appropriate steps to remediate identified vulnerabilities.

- a. Any critical or high-risk vulnerability that is associated with a Security Incident shall be remediated within forty-eight (48) hours of the identification of the vulnerability. If the vulnerability cannot be remediated as indicated above, then Defendant shall within forty-eight (48) hours of the identification of such vulnerability take the application or system affected by such vulnerability offline until such vulnerability is remediated.

24. Software Updates and Patch Management: Defendant shall implement and maintain a reasonable policy to update and patch software on its network.

Defendant shall employ processes and procedures to ensure the timely scheduling and installation of any security update or patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the Defendant's network, the impact on Defendant's operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by a U.S. government authority.

25. Segmentation: Defendant shall implement and maintain policies and procedures designed to appropriately segment its network, which shall, at a minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

26. Encryption: Defendant shall Encrypt PI and ePHI at rest and in transit as appropriate, and in accordance with applicable law.

27. Logging and Monitoring: Defendant shall implement and maintain reasonable controls to centralize logging and monitoring of Defendant's network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. Defendant shall ensure that logs of system activity are regularly reviewed and analyzed, that logs are protected from unauthorized access or deletion, and that appropriate follow-up and remediation steps are taken with respect to any Security Incident.

28. Intrusion Detection and Prevention: Defendant shall implement and maintain intrusion detection and prevention tools, including but not limited to

firewalls and antivirus/antimalware software.

29. Penetration Testing: Defendant shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities. Such testing shall occur at least every eighteen (18) months and shall include penetration testing of Defendant's internal and external network defenses. Defendant shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation. Defendant shall document the penetration test results and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

Assessment and Reporting Requirements

30. HIPAA Risk Analysis and Risk Management Plan: Defendant shall obtain an annual risk assessment by a qualified, independent third party, which shall, at a minimum, include: the identification of internal and external risks to the security, confidentiality, or integrity of PHI or ePHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information; an assessment of the safeguards in place to control these risks; an evaluation and adjustment of the WISP considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and documentation of safeguards implemented in response to such risk assessments. Defendant shall document the risk assessments and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon

request.

31. Information Security Program Assessment: Defendant shall, within one hundred and eighty (180) days of the Effective Date, and thereafter biennially for a period of six (6) years, submit to an assessment of its compliance with this Consent Judgment by a qualified, independent third party (“Assessor”). Following each such assessment, the Assessor shall prepare a report including its findings and recommendations (“Security Report”), a copy of which shall be provided to the Indiana Attorney General within forty-five days (45) of its completion.

- a. Within one hundred and twenty (120) days of receipt of each Security Report, Defendant shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report.
- b. Within one hundred eighty (180) days of Defendant’s receipt of each Security Report, Defendant shall forward to the Indiana Attorney General a description of any action Defendant takes and, if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

Payment to the State

32. Within thirty (30) days of the Effective Date, Defendant shall pay One Hundred and Twenty-Five Thousand Dollars (\$125,000.00) to the Office of the Indiana Attorney General, to be used for any purpose allowable under Indiana law. For purposes of IRS Form 1098-F, all payments shall be reported in Box 2 as “Amount

to be paid for violation or potential violation.” To effectuate this payment and reporting, the State shall provide Defendant with an IRS Form W-9 and ACH instructions, and Defendant shall provide the State with an IRS Form W-9 upon execution of this Consent Judgment.

Release

33. Following full payment of the amount due by Defendant under this Consent Judgment, the State shall release and discharge Defendant from all civil claims that the State could have brought under the Relevant Laws, based on Defendant’s conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the State to enforce the obligations that Defendant or its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Consent Judgment. Further, nothing in the Consent Judgment shall be construed to create, waive, or limit any private right of action.

34. Notwithstanding any term of this Consent Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 33 above as to any entity or person, including Defendant:

- a. Any criminal liability that any person or entity, including Defendant, has or may have;
- b. Any civil liability or administrative liability that any person or entity, including Defendant, has or may have under any statute, regulation, or rule not expressly covered by the release in Paragraph 33 above,

including but not limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

Consequences of Noncompliance

35. Defendant represents that it has fully read this Consent Judgment and understands the legal consequences attendant to entering into this Consent Judgment. Defendant understands that any violation of this Consent Judgment may result in the State seeking all available relief to enforce this Consent Judgment, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other relief provided by the laws of the State or authorized by a court. If the State is required to file a petition to enforce any provision of this Consent Judgment against Defendant, Defendant agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Consent Judgment against such Defendant.

General Provisions

36. Any failure of the State to exercise any of its rights under this Consent Judgment shall not constitute a waiver of any rights hereunder.

37. Defendant hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Consent Judgment. Defendant is and has been represented by legal counsel and has been advised by its legal counsel of the meaning and legal effect of this Consent Judgment.

38. This Consent Judgment shall bind Defendant and its officers, subsidiaries, affiliates, agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

39. Defendant shall deliver a copy of this Consent Judgment to its executive management having decision-making authority with respect to the subject matter of this Consent Judgment within thirty (30) days of the Effective Date.

40. The settlement negotiations resulting in this Consent Judgment have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Consent Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

41. Defendant waives notice and service of process for any necessary filing relating to this Consent Judgment, and the Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enforcing and modifying this Consent Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Consent Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Consent Judgment is filed, and then only to the extent specifically set forth in such Consent Judgment. The Parties may agree in writing, through counsel, to an extension of any time period specified in this Consent Judgment without a court order.

42. Defendant does not object to *ex parte* submission and presentation of this Consent Judgment by the Plaintiff to the Court, and does not object to the Court's

approval of this Consent Judgment and entry of this Consent Judgment by the Clerk of the Court.

43. The Parties agree that this Consent Judgment does not constitute an approval by the State of any of Defendant's past or future practices, and Defendant shall not make any representation to the contrary.

44. The requirements of the Consent Judgment are in addition to, and not in lieu of, any other requirements of federal or state law. Nothing in this Consent Judgment shall be construed as relieving Defendant of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of the Consent Judgment be deemed as permission for Defendant to engage in any acts or practices prohibited by such laws, regulations, or rules.

45. This Consent Judgment shall not create a waiver or limit Defendant's legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Consent Judgment or to demonstrate that Defendant was on notice as to the allegations contained herein.

46. This Consent Judgment shall not waive Defendant's right to defend itself, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Consent Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Consent Judgment.

47. This Consent Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendant may have in connection with any investigations, claims, or other matters not released in this Consent Judgment.

48. Defendant shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Consent Judgment or for any other purpose which would otherwise circumvent any part of this Consent Judgment.

49. If any clause, provision, or section of this Consent Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Consent Judgment and this Consent Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

50. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Consent Judgment.

51. To the extent that there are any, Defendant agrees to pay all court costs associated with the filing of this Consent Judgment.

52. The orders contained in this Consent Judgment shall be effective for six (6) years following the Effective Date.

Notices

53. Any notices or other documents required to be sent to the Parties pursuant to the Consent Judgment shall be sent by (A) email; and (B) United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. The required notices and/or documents shall be sent to:

a. For the State:

Douglas S. Swetnam
Section Chief – Data Privacy & Identity Theft Unit
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
douglas.swetnam@atg.in.gov

Jennifer M. Van Dame
Deputy Attorney General
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
jennifer.vandame@atg.in.gov

b. For Defendant:

Kevin Scott
Shareholder
Greenberg Traurig, LLP
77 W Wacker Dr
Suite 3100
Chicago, IL 60601
Kevin.scott@gtlaw.com

IT IS STIPULATED:

FOR THE STATE OF INDIANA


Office of Indiana Attorney General

By 

Date: 11/01/2023

Jennifer M. Van Dame
Attorney No. 32788-53
Deputy Attorney General
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037

FOR DEFENDANT

By 

Date: 10/30/23

Dennis P. Han
Managing Partner
CarePointe, P.C.
99 East 86th Avenue, Suite A
Merriville, IN 46410

By 

Date: 30 October 2023

Kevin Scott
Shareholder
Greenberg Traurig, LLP
77 W Wacker Dr, Suite 3100
Chicago, IL 60601

SO ORDERED, ADJUDGED, AND DECREED:

By _____
JUDGE

Date: _____

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
NEW ALBANY DIVISION

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

JACKSON COUNTY SCHNECK
MEMORIAL HOSPITAL d/b/a
SCHNECK MEDICAL CENTER,

Defendant.

CASE NO. 4:23-cv-0155

COMPLAINT

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by Deputy Attorney General Jennifer M. Van Dame, brings this action for injunctive relief, statutory damages, attorney fees, and costs against Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”).

I. PARTIES, JURISDICTION, AND VENUE

1. The Indiana Attorney General is authorized to bring this action to enforce HIPAA pursuant to 42 U.S.C. § 1320d-5(d). The Indiana Attorney General is authorized to bring this action to enforce the DSBA pursuant to Ind. Code § 24-4.9-4-2, and the DCSA pursuant to Ind. Code § 24-5-0.5-4(c).

2. Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center (“SMC”) is an Indiana county hospital with a principal office located at 411 W. Tipton Street, Seymour, IN 47274.

3. This Court has jurisdiction pursuant to 42 U.S.C. § 1320d-5(d)(1) and 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C § 1367.

4. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2).

5. The State has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. §1320d-5(d)(4).

II. FACTUAL ALLEGATIONS

6. At all times relevant to this Complaint, SMC provided health care services to Indiana residents and was a covered entity within the meaning of HIPAA. *See* 45 C.F.R. § 160.103.

7. On or around September 29, 2021, an unauthorized third party (the “threat actor”) executed a ransomware attack on SMC’s systems and exfiltrated data from SMC’s systems (the “Data Breach”).

8. SMC states on its website that it is “Committed to protecting your privacy.” Further, SMC’s Notice of Health Information Privacy Practices (effective September 22, 2013), available at <https://www.schneckmed.org/privacy-policy> (“Notice of Privacy Practices”), states:

- a. “We understand that medical information about you and your health is personal. We are committed to protecting medical information about you.”
- b. “We are required by law to . . . ensure that medical information identifying you is kept private[.]”

9. Notwithstanding SMC’s representations regarding its commitment to patient privacy on its website and in its Notice of Privacy Practices, a HIPAA risk analysis completed in December 2020 put SMC on notice of many critical security issues that contributed to the Data Breach the following year. SMC had actual knowledge of and failed to address these security issues.

10. The Data Breach exposed the personal information and/or protected health information (“PHI”) of approximately 89,707 Indiana residents.

11. The categories of personal information and/or PHI exposed by the Data Breach included: full names, addresses, dates of birth, Social Security numbers, driver’s license numbers, financial account information, payment card information, medical diagnosis and conditions information, and health insurance information.

12. On September 29, 2021, SMC released a generic statement on its

website indicating SMC had “learned that it was a victim of a cyberattack that affected organizational operations” but failed to disclose the risk of exposure to patient information or encourage patients to take precautions to mitigate the risk of identity theft or fraud, despite SMC knowing at that time that a large amount of data had been exfiltrated from its systems.

13. SMC released another statement on November 26, 2021, referencing the threat actor’s exfiltration of files but failing to disclose that PHI was exposed during the incident, despite SMC knowing at that time that data had been exfiltrated from a system used to transmit PHI.

14. Ultimately, SMC failed to provide direct notification to patients until May 13, 2022, two hundred and twenty-six (226) days after SMC first discovered the Data Breach.

15. The May 13, 2022 notification was the first public statement in which SMC acknowledged the Data Breach involved PHI, despite SMC knowing since at least November 26, 2021, that data was exfiltrated from a system that contained PHI.

16. Further, in the substitute notice posted on SMC’s website on May 13, 2022, SMC misrepresented that it “discovered **on March 17, 2022** that one or more of the files removed by the unauthorized party on or about September 29, 2021 contained protection health information.” (Emphasis added.)

III. HIPAA BACKGROUND

17. As a covered entity, SMC was required to comply with the HIPAA standards that govern the security and privacy of PHI and notification to patients in the event of a breach. *See* 45 C.F.R. Part 164.

18. The HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) requires covered entities to ensure the confidentiality, integrity, and availability of all PHI that the covered entity creates, receives, maintains, or transmits and to protect against any reasonably anticipated threats to the security or integrity of such information. *See* 45 C.F.R. § 164.306. To this end, the HIPAA Security Rule requires covered entities to employ appropriate administrative, physical, and technical safeguards to maintain the security and integrity of PHI. *See* 45 C.F.R. §§ 164.308, 164.310, 164.312.

19. The HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D) requires covered entities to timely notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as a result of a breach. Notification must be provided “without unreasonable delay and **in no case later than 60 calendar days** after the discovery of a breach.” 45 C.F.R. § 164.404(b) (emphasis added). “[A] breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity.” 45 C.F.R. § 164.404(a)(2). Importantly, “Under this rule, the time

period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule.” 78 Fed. Reg. 5648.

20. Finally, the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) prohibits covered entities from using or disclosing PHI, except as permitted by HIPAA.

IV. CAUSES OF ACTION

COUNT ONE: FAILURE TO COMPLY WITH HIPAA SECURITY RULE

21. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

22. SMC failed to employ appropriate safeguards to maintain the security and integrity of PHI, including as follows:

- a. SMC failed to implement, review, and/or modify policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §§ 164.308(a)(1)(i) and 164.306(e);
- b. SMC failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by SMC in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);
- c. SMC failed to implement a risk management plan with security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B);

- d. SMC failed to implement procedures for guarding against, detecting, and reporting malicious software, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(B);
- e. SMC failed to implement procedures for monitoring log-ins, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(C);
- f. SMC failed to implement procedures for creating, changing, and safeguarding passwords, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);
- g. SMC failed to implement technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons that have been granted access rights, including assignment of unique names and/or numbers for identifying and tracking user identity in violation of 45 C.F.R. § 164.312(a)(1)-(a)(2)(i);
- h. SMC failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain PHI in violation of 45 C.F.R. § 164.312(b);
- i. SMC failed to implement procedures to verify that a person seeking access to PHI is the one claimed in violation of 45 C.F.R. § 164.312(d);
and

- j. SMC failed to implement policies and procedures to address security incidents – i.e. to respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents in violation of 45 C.F.R. § 164.308(a)(6).

**COUNT TWO:
FAILURE TO COMPLY WITH HIPAA BREACH NOTIFICATION RULE**

23. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

24. SMC was required to provide direct notification to patients “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.” 45 C.F.R. § 164.404(b).

25. Because SMC discovered the Data Breach on September 29, 2021, SMC was required to provide direct notification to patients no later than November 28, 2021.

26. SMC failed to provide direct notification to patients until May 13, 2022, two hundred and twenty-six (226) days after SMC first discovered the Data Breach.

27. SMC’s notification to patients was unreasonably delayed and untimely, in violation of 45 C.F.R. § 164.404.

**COUNT THREE:
FAILURE TO COMPLY WITH HIPAA PRIVACY RULE**

28. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

29. As a covered entity, SMC was prohibited from disclosing PHI except as permitted by HIPAA. 45 C.F.R. § 164.502(a).

30. HIPAA defines “disclosure” as “the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.” 45 C.F.R. § 160.103.

31. SMC’s poor security practices subjected the PHI of approximately 89,707 Indiana residents to disclosure during the Data Breach.

32. The disclosures were not permitted under any HIPAA exception.

33. Each disclosure violated 45 C.F.R. § 164.502.

**COUNT FOUR:
FAILURE TO IMPLEMENT AND MAINTAIN
REASONABLE PROCEDURES IN VIOLATION OF
INDIANA DISCLOSURE OF SECURITY BREACH ACT**

34. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

35. The DSBA requires a data base owner to “implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.” Ind. Code § 24-4.9-3-3.5(c).

36. The DSBA defines “personal information” to include:

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual’s first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver’s license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Ind. Code § 24-4.9-2-10.

37. The categories of personal information exposed by the Data Breach included full names, Social Security numbers, driver's license numbers, financial account information, and payment card information.

38. SMC violated the DSBA by failing to implement and maintain reasonable security procedures to protect and safeguard personal information of Indiana residents.

39. SMC is not exempt from the DSBA because SMC was not in compliance with HIPAA at the times relevant to this Complaint. *See* Ind. Code § 24-4.9-3-3.5(a).

**COUNT FIVE:
VIOLATIONS OF INDIANA DECEPTIVE CONSUMER SALES ACT**

40. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

41. The DCSA regulates unfair, abusive, and/or deceptive acts, omissions, and/or practices between suppliers and consumers engaging in consumer transactions. *See* Ind. Code § 24-5-0.5-3.

42. Under the DCSA, a "consumer transaction" includes services and other intangibles. Ind. Code § 24-5-0.5-2(a)(1).

43. In supplying Indiana patients with health care services, SMC was and remains involved in consumer transactions in Indiana and is a "supplier" as defined by Ind. Code § 24-5-0.5-2(a)(3).

44. The DCSA prohibits a supplier from committing “an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.” Ind. Code. § 24-5-0.5-3(a).

45. It is a deceptive act under the DCSA to represent to consumers that the subject of a consumer transaction “has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have,” or “is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.” Ind. Code § 24-5-0.5-3(b)(1)-(2).

46. On its website and Notice of Privacy Practices, SMC represented to patients that it is committed to “protecting your privacy” and “protecting medical information about you.” SMC also implicitly represented that it was compliant with HIPAA and other applicable laws by stating: “We are required by law to . . . ensure that medical information identifying you is kept private[.]”

47. Contrary to these representations, SMC knowingly failed to implement and maintain reasonable security practices to protect patients’ personal information and PHI. SMC also knowingly failed to comply with HIPAA by failing to address the security issues flagged in the December 2020 HIPAA risk analysis.

48. SMC explicitly and implicitly misrepresented that its systems were secure and compliant, when SMC knew they were not.

49. In the substitute notice posted on SMC's website on May 13, 2022, SMC also misrepresented that it "discovered on March 17, 2022 that one or more of the files removed by the unauthorized party . . . contained protection health information." In fact, SMC knew since at least November 26, 2021, that data was exfiltrated from a system that contained PHI.

V. PRAYER FOR RELIEF

WHEREFORE, the State of Indiana respectfully requests that this Court enter judgment against SMC and in favor of the State as follows:

- a. Finding that SMC violated HIPAA, DSBA, and DCSA by engaging in the unlawful acts and practices alleged herein, and permanently enjoining SMC from continuing to engage in such unlawful acts and practices pursuant to 42 U.S.C. § 1320d-5(d)(1)(A), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c);
- b. Ordering SMC to pay statutory damages of \$100 per HIPAA violation, as provided by 42 U.S.C. § 1320d-5(d)(2);
- c. Ordering SMC to pay a \$5,000 civil penalty for violating the DSBA, as provided by Ind. Code § 24-4.9-3-3.5(f);
- d. Ordering SMC to pay a \$5,000 civil penalty for each knowing violation of the DCSA alleged herein, as provided by Ind. Code § 24-5-0.5-4(g);
- e. Ordering SMC to pay all costs and fees for the investigation and prosecution of this action pursuant to 42 U.S.C. § 1320d-5(d)(3), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c); and
- f. Granting any such further relief as the Court may deem appropriate.

Respectfully submitted,

STATE OF INDIANA EX REL.
INDIANA ATTORNEY GENERAL
TODD ROKITA

Date: September 6, 2023

By:



Jennifer M. Van Dame
Indiana Attorney No. 32788-53
Deputy Attorney General
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037
Phone: 317-232-0486
Fax: 317-232-7979
Email: jennifer.vandame@atg.in.gov

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
NEW ALBANY DIVISION**

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

JACKSON COUNTY SCHNECK
MEMORIAL HOSPITAL d/b/a
SCHNECK MEDICAL CENTER,

Defendant.

Case No. 4:23-cv-00155-KMB-SEB

REVISED CONSENT JUDGMENT AND ORDER

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by counsel, Deputy Attorney General Jennifer M. Van Dame, and Defendant, Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center (“SMC”) (collectively, the “Parties”), have agreed to the Court’s entry of this Revised Consent Judgment and Order (“Consent Judgment”) without trial or adjudication of any issue of fact or law.

This Consent Judgment resolves the Plaintiff’s investigation of the data breach described in the Complaint filed in this action regarding SMC’s compliance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and Department of

Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”) (collectively, the “Relevant Laws”).

This Consent Judgment is not intended and shall not be used or construed as an admission by Defendant of any violation of the Relevant Laws, nor shall it be construed as an abandonment by the State of its allegations that Defendant violated the Relevant Laws.

The Parties consent to entry of this Consent Judgment by the Court as a final determination and resolution of the issues alleged in the Complaint.

THE PARTIES

1. The Office of the Indiana Attorney General (“OAG”) is charged with enforcement of the Relevant Laws, including HIPAA pursuant to 42 U.S.C. § 1320d-5(d).

2. Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center (“SMC”) is an Indiana county hospital with a principal office located at 411 W. Tipton Street, Seymour, IN 47274.

BACKGROUND

3. On or around September 29, 2021, SMC experienced a data breach that exposed the Personal Information and/or Protected Health Information of approximately 89,707 Indiana residents.

4. The OAG investigated this incident pursuant to the Relevant Laws.

STIPULATIONS

5. The Parties agree to and do not contest the entry of this Consent Judgment.

6. At all times relevant to this matter, SMC was engaged in trade and commerce affecting consumers in the State of Indiana insofar as SMC provided health care services to consumers in Indiana. SMC was also in possession of the Personal Information and Protected Health Information of Indiana residents.

7. At all times relevant to this matter, SMC was a Covered Entity subject to the requirements of HIPAA.

8. The Parties consent to jurisdiction and venue in this Court for purposes of entry of this Consent Judgment as well as for the purpose of any subsequent action to enforce it.

JURISDICTION

9. The Court finds that it has jurisdiction over the Parties for purposes of entry of this Consent 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 of this Consent Judgment pursuant to 42 U.S.C. § 1320d-5(d), 28 U.S.C. § 1331, and 28 U.S.C. § 1367 for the purpose of entering and enforcing the Consent Judgment, and venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1). 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 Consent Judgment.

ORDER

NOW THEREFORE, the Court has reviewed the terms of this Consent Judgment and based upon the Parties' agreement and for good cause shown, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED AS FOLLOWS:

DEFINITIONS

11. For the purposes of this Consent Judgment, the following definitions shall apply:

- a. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 meaning "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information."
- b. "Breach" shall be defined in accordance with 45 C.F.R. § 164.402 to mean "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." The definition of "breach" shall also include all exclusions listed in 45 C.F.R. § 164.402(1) and (2).

- c. “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103.
- d. “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103 meaning “a health plan, health care clearinghouse, or health care provider that transmits health information in electronic form in connection with a transaction” covered by Subchapter C *Administrative Data Standards and Related Requirements*.
- e. “DCSA” means the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.*, and any related statutes and rules adopted pursuant thereto in effect on or prior to May 13, 2022. The DCSA is incorporated fully herein including all terms and definitions set forth therein.
- f. “DSBA” means the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.*, and any related statutes and rules adopted pursuant thereto in effect on or prior to May 13, 2022. The DSBA is incorporated fully herein including all terms and definitions set forth therein.
- g. “Effective Date” shall mean the date on which this Consent Judgment is approved by the Court.
- h. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- i. “Encrypt” or “Encryption” shall mean to render unreadable, indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally by the National

Institute of Standards and Technology (“NIST”).

- j. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and any related Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* HIPAA is incorporated fully herein including all terms and definitions set forth therein.
- k. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).
- l. “Personal Information” or “PI” shall be defined in accordance with DSBA, Ind. Code § 24-4.9-2-10.
- m. “Privacy Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ medical records and other Protected Health Information, including ePHI, that is created, received, used, or maintained by a Covered Entity or Business Associate that

performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

- n. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- o. “Security Incident” shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.
- p. “Security Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ Electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.
- q. “Technical Safeguards” shall be defined in accordance with 45 C.F.R. § 164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

INJUNCTIVE PROVISIONS

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE COMPLIANCE WITH THE LAW:

Compliance with Federal and State Laws

8. Defendant shall comply with the HIPAA Privacy and Security Rules and shall implement all Administrative and Technical Safeguards required by HIPAA.

9. To the extent applicable to the Defendant, the Defendant shall comply with DSBA and DCSA in connection with its collection, maintenance, and safeguarding of PI, PHI, and ePHI.

10. Defendant shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which Defendant maintains and/or protects the privacy, security, confidentiality, or integrity of PI, PHI, or ePHI.

11. Defendant shall comply with the breach notification requirements of DSBA and HIPAA, as applicable.

Information Security Program

12. Overview: Within ninety (90) days after the Effective Date, Defendant shall develop, implement, and maintain an information security program (“Information Security Program” or “Program”) that shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendant’s operations; (ii) the nature and scope of Defendant’s activities; and (iii) the sensitivity of the personal information that Defendant maintains. At a minimum, the Program shall include the Specific Technical Safeguards and Controls in Paragraphs 18 through 31 below. Defendant may satisfy the requirements to implement and maintain the Program through review, maintenance, and as necessary, updating of an existing information security program

and related safeguards, provided that such program and safeguards meet the requirements of this Consent Judgment. Defendant shall provide the resources and support necessary to fully implement the Program so that it functions as required and intended by this Consent Judgment.

13. Governance: Defendant shall designate an executive or officer whose responsibility will be to implement, maintain, and monitor the Program (hereinafter referred to as the “Chief Information Officer” or “CIO”). The CIO shall have appropriate training, expertise, and experience to oversee the Program and shall regularly report to the Board of Directors (“Board”) and Chief Executive Officer (“CEO”) regarding the status of the Program, the security risks faced by the Defendant, resources required for implementation of the Program, and the security implications of Defendant’s business decisions. At a minimum, the CIO shall report any future Security Incident in accordance with the Plan identified in Paragraph 14.

14. Incident Response Plan: Defendant shall implement and maintain a written incident response plan (“Plan”) to prepare for and respond to any future Breaches. Defendant shall review and update the Plan as necessary. At a minimum, the Plan shall provide for the following phases:

- a. Preparation;
- b. Detection and Analysis;
- c. Containment;
- d. Notification and Coordination with Law Enforcement;
- e. Eradication;

- f. Recovery;
 - g. Consumer and Regulator Notification; and
 - h. Post-Incident Analysis and Remediation.
15. Table-Top Exercises: Defendant shall conduct, at a minimum, biannual incident response plan exercises to test and assess its preparedness to respond to Security Incidents and Breaches.
16. Training: Within ninety (90) days of the Effective Date, and at least annually thereafter, Defendant shall provide data security and privacy training to all personnel with access to PI, PHI, or ePHI. Defendant shall provide this training to any employees newly hired to, or transitioned into, a role with access to PI, PHI, or ePHI, within thirty (30) days of hire or transition. Such training shall be appropriate to employees' job responsibilities and functions. Defendant shall document the trainings and the date(s) upon which they were provided.
17. Minimum Necessary Standard: Defendant shall design and update the Program consistent with the Minimum Necessary Standard.

Specific Technical Safeguards and Controls

18. Password Management: Defendant shall implement and maintain password policies and procedures requiring the use of strong, complex passwords with reasonable password-rotation requirements and ensuring that stored passwords are protected from unauthorized access.
19. Account Management: Defendant shall implement and maintain policies and procedures to manage, and limit access to and use of, all accounts with

access to PI or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Defendant shall not permit use of shared accounts with access to PI or ePHI.

20. Access Controls: Defendant shall implement and maintain policies and procedures to ensure that access to PI and ePHI is granted under the principle of least privilege. Such policies and procedures shall further include a means to regularly review access and access levels of users and remove network and remote access within twenty-four (24) hours of notification of termination for any employee whose employment has ended.

21. Multi-Factor Authentication: Defendant shall require the use of multi-factor authentication for remote access to Defendant's systems. Such multi-factor authentication methods should not include telephone or SMS-based authentication methods, but can include mobile applications, physical security keys, or other more secure options.

22. Asset Inventory: Defendant shall regularly inventory and classify all assets that comprise Defendant's network. The asset inventory shall, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the network; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores PI or ePHI; and (g) each security update or patch applied or installed during the preceding period.

23. Vulnerability Scanning: Defendant shall conduct regular vulnerability scanning using industry-standard tool and shall take appropriate steps to remediate

identified vulnerabilities.

- a. Any vulnerability that is associated with a Security Incident shall be remediated within forty-eight (48) hours of the identification of the vulnerability. If the vulnerability cannot be remediated within forty-eight (48) hours of its identification, Defendant shall implement compensating controls or decommission the system within forty-eight (48) hours of the identification of the vulnerability. Defendant shall maintain documentation regarding the analysis of the vulnerabilities and timeline for remediation, compensating controls and/or documentation why remediation is not available.

24. Software Updates and Patch Management: Defendant shall implement and maintain a policy to update and patch software on its network.

- a. Defendant shall employ processes and procedures to ensure the timely scheduling and installation of any security update or patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the Defendant's network, the impact on Defendant's operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by a U.S. government authority.
- b. In connection with the scheduling and installation of any update and/or patch rated critical or high, Defendant shall verify that the update and/or patch was applied and installed successfully throughout the

network.

25. Segmentation: Defendant shall implement and maintain policies and procedures designed to appropriately segment its network, which shall, at a minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

26. Encryption: Defendant shall Encrypt PI and ePHI at rest and in transit as appropriate, and in accordance with applicable law.

27. Logging and Monitoring: Defendant shall implement and maintain reasonable controls to centralize logging and monitoring of Defendant's network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. Defendant shall ensure that logs of system activity are regularly and actively reviewed and analyzed in as close to real-time as possible, that logs are protected from unauthorized access or deletion, and that appropriate follow-up and remediation steps are taken with respect to any Security Incident.

28. Intrusion Detection and Prevention: Defendant shall implement and maintain intrusion detection and prevent tools, including but not limited to firewalls and antivirus/antimalware software.

29. Penetration Testing: Defendant shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities. Such testing shall occur on at least an

annual basis and shall include penetration testing of Defendant's internal and external network defenses. Defendant shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation. Defendant shall document the penetration test results and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

30. HIPAA Risk Analysis and Risk Management Plan: Defendant shall obtain an annual risk assessment by a qualified, independent third party, which shall, at a minimum, include: the identification of internal and external risks to the security, confidentiality, or integrity of PHI or ePHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information; an assessment of the safeguards in place to control these risks; an evaluation and adjustment of the Program considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and documentation of safeguards implemented in response to such annual risk assessments. Defendant shall document the risk assessments and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

31. Information Security Program Assessment: Defendant shall, within one hundred and eighty (180) days of the Effective Date, and thereafter biennially for a period of seven (7) years, submit to an assessment of its compliance with this Consent Judgment by a qualified, independent third party ("Assessor"). Following each such

assessment, the Assessor shall prepare a report including its findings and recommendations (“Security Report”), a copy of which shall be provided to the Indiana Attorney General within thirty days (30) of its completion.

- a. Within ninety (90) days of receipt of each Security Report, Defendant shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report.
- b. Within one hundred eighty (180) days of Defendant’s receipt of each Security Report, Defendant shall forward to the Indiana Attorney General a description of any action Defendant takes and, if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

Payment to the State

32. Within thirty (30) days of the Effective Date, Defendant shall pay Two Hundred Fifty Thousand Dollars (\$250,000.00) to the Office of the Indiana Attorney General, to be used for any purpose allowable under Indiana law. For purposes of IRS Form 1098-F, all payments shall be reported in Box 2 as “Amount to be paid for violation or potential violation.” To effectuate this payment and reporting, the State shall provide Defendant with an IRS Form W-9 and ACH instructions, and Defendant shall provide the State with an IRS Form W-9 upon execution of this Consent Judgment.

Release

33. Following full payment of the amount due by Defendant under this Consent Judgment, the State shall release and discharge Defendant from all civil claims that the State could have brought under the Relevant Laws, based on Defendant's conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the State to enforce the obligations that Defendant or its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Consent Judgment. Further, nothing in the Consent Judgment shall be construed to create, waive, or limit any private right of action.

34. All obligations under this Consent Judgment shall expire seven (7) years from the effective date.

35. Notwithstanding any term of this Consent Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 33 above as to any entity or person, including Defendant:

- a. Any criminal liability that any person or entity, including Defendant, has or may have;
- b. Any civil liability or administrative liability that any person or entity, including Defendant, has or may have under any statute, regulation, or rule not expressly covered by the release in Paragraph 33 above, including but not limited to, any and all of the following claims: (i) State

or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

Consequences of Noncompliance

36. Defendant represents that it has fully read this Consent Judgment and understands the legal consequences attendant to entering into this Consent Judgment. Defendant understands that any violation of this Consent Judgment may result in the State seeking all available relief to enforce this Consent Judgment, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other relief provided by the laws of the State or authorized by a court. If the State is required to file a petition to enforce any provision of this Consent Judgment against Defendant, Defendant agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Consent Judgment against such Defendant.

General Provisions

37. Any failure of the State to exercise any of its rights under this Consent Judgment shall not constitute a waiver of any rights hereunder.

38. Defendant hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Consent Judgment. Defendant is and has been represented by legal counsel and has been advised by its legal counsel of the meaning and legal effect of this Consent Judgment.

39. This Consent Judgment shall bind Defendant and its officers, subsidiaries, affiliates, agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

40. Defendant shall deliver a copy of this Consent Judgment to its executive management having decision-making authority with respect to the subject matter of this Consent Judgment within thirty (30) days of the Effective Date.

41. The settlement negotiations resulting in this Consent Judgment have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Consent Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

42. Defendant waives notice and service of process for any necessary filing relating to this Consent Judgment, and the Court retains jurisdiction over this Consent Judgment and the Parties hereto for the purpose of enforcing and modifying this Consent Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Consent Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Consent Judgment is filed, and then only to the extent specifically set forth in such Consent Judgment. The Parties may agree in writing, through counsel, to an extension of any time period specified in this Consent Judgment without a court order.

43. Defendant does not object to *ex parte* submission and presentation of this Consent Judgment by the Plaintiff to the Court, and do not object to the Court's

approval of this Consent Judgment and entry of this Consent Judgment by the Clerk of the Court.

44. The Parties agree that this Consent Judgment does not constitute an approval by the State of any of Defendant's past or future practices, and Defendant shall not make any representation to the contrary.

45. The requirements of the Consent Judgment are in addition to, and not in lieu of, any other requirements of federal or state law. Nothing in this Consent Judgment shall be construed as relieving Defendant of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of the Consent Judgment be deemed as permission for Defendant to engage in any acts or practices prohibited by such laws, regulations, or rules.

46. This Consent Judgment shall not create a waiver or limit Defendant's legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Consent Judgment or to demonstrate that Defendant was on notice as to the allegations contained herein.

47. This Consent Judgment shall not waive Defendant's right to defend itself, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Consent Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Consent Judgment.

48. This Consent Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendant may have in connection with any investigations, claims, or other matters not released in this Consent Judgment.

49. Defendant shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Consent Judgment or for any other purpose which would otherwise circumvent any part of this Consent Judgment.

50. If any clause, provision, or section of this Consent Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Consent Judgment and this Consent Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

51. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Consent Judgment.

52. To the extent that there are any, Defendant agrees to pay all court costs associated with the filing of this Consent Judgment.

Notices

53. Any notices or other documents required to be sent to the Parties pursuant to the Consent Judgment shall be sent by (A) email; and (B) United States

Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. The required notices and/or documents shall be sent to:

a. For the State:

Douglas S. Swetnam
Section Chief – Data Privacy & Identity Theft Unit
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
douglas.swetnam@atg.in.gov

Jennifer M. Van Dame
Deputy Attorney General
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
jennifer.vandame@atg.in.gov

b. For Defendant:

James Giszczak
McDonald Hopkins
39533 Woodward Avenue, Suite 318
Bloomfield Hills, MI 48304
jgiszczak@mcdonaldhopkins.com

IT IS STIPULATED:

FOR THE STATE OF INDIANA

Office of Indiana Attorney General



By _____

Date: 10/17/2023

Jennifer M. Van Dame
Attorney No. 32788-53
Deputy Attorney General
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037
Phone: 317-232-0486
jennifer.vandame@atg.in.gov

FOR DEFENDANT



By _____
Eric D. Fish, MD, President/CEO

Date: ___October 19, 2023___



By _____

Date: ___October 20, 2023___

Heather M. Shumaker
Indiana Attorney No. 28340-49
McDonald Hopkins LLP
39533 Woodward Avenue, Suite 318
Bloomfield Hills, MI 48304
Phone: 248-402-4066
hshumaker@mcondaldhopkins.com

SO ORDERED, ADJUDGED, AND DECREED:

By _____ Date: _____
JUDGE

Service will be made electronically on all ECF-registered counsel of record via email generated by the court's ECF system.

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
Indianapolis Division**

STATE OF INDIANA <i>ex rel.</i> ATTORNEY)		
GENERAL OF INDIANA,))	
)	
Plaintiff,))	
)	CIVIL ACTION NO. 1:20-cv-1616
v.))	
)	
DXC TECHNOLOGY SERVICES, LLC,))	
)	
Defendant.))	

COMPLAINT

I. PRELIMINARY STATEMENT

1. The Plaintiff, State of Indiana, by and through its Attorney General, for the residents of the State of Indiana and on behalf of the State of Indiana in its sovereign capacity, by counsel Douglas S. Swetnam, Deputy Attorney General, institutes this action for injunctive relief, statutory damages, attorneys’ fees, and the costs of this action against DXC Technology Services, LLC (“DXC”), alleging violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, and Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively referred to as “HIPAA”).

II. JURISDICTION AND VENUE

2. The Court has jurisdiction for this cause of action pursuant to 42 U.S.C. § 1320d-5(d) and 28 U.S.C. § 1331.

3. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(2), (c) and (d).

4. Plaintiff, Attorney General of the State of Indiana, has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. § 1320d-5(d)(4).

III. PARTIES

5. Plaintiff, Attorney General of the State of Indiana, is authorized to bring this action and to seek injunctive and other statutory relief pursuant to 42 U.S.C. § 1320d-5(d)(1).

6. At all times relevant to this Complaint, DXC was a Virginia limited liability company with a principal office at 1775 Tysons Blvd., 9th Floor, Tysons Corner, Virginia 22102.

7. At all times relevant to this Complaint, DXC was engaged in business in Indiana as a contractor for the Indiana Family and Social Services Administration (“FSSA”), operating the CoreMMIS Provider Healthcare Portal (“Portal”).

IV. FACTUAL ALLEGATIONS

8. At all times relevant to this Complaint, FSSA provided healthcare services to Indiana residents and was a covered entity within the meaning of HIPAA.

9. By operating the Portal for FSSA, DXC is a business associate within the meaning of 45 C.F.R. § 160.103.

10. As a business associate of FSSA, DXC created or received protected health information (“PHI”), which primarily included electronic PHI (“ePHI”), both of which are defined by 45 C.F.R. § 160.103. The ePHI was stored in the Portal.

11. On or about May 10, 2017, DXC identified a vulnerability in the Portal that allowed unauthenticated access to ePHI, specifically, remittance advices.

12. Remittance advices are reports containing patients’ names, Medicaid Identification numbers, patient numbers, provider information, procedure codes, dates of service, and payment amounts. Said reports are meant for viewing by FSSA and authorized health care providers only.

13. The vulnerability in the Portal allowed anyone performing a search using a public search engine, such as Google, Yahoo, or Bing, to access direct links to remittance advices without

providing authentication. Without these direct links, it is extremely unlikely that someone could access the remittance advices in the Portal.

14. Subsequent investigation determined that the vulnerability existed from on or about February 13, 2017 to the date of discovery, May 10, 2017.

15. Beginning on or about March 22, 2017, automated web crawlers entered the Portal. A web crawler is a program or automated script which browses the internet in a methodical, automated manner. Search engines employ web crawlers to visit websites and read their pages and other information in order to index or create entries for search results. Source: <https://searchmicroservices.techtarget.com/definition/crawler>, last visited December 16, 2019.

16. Subsequent forensic investigation determined that the web crawlers indexed specific links corresponding to at least 1,337 remittance advices containing the ePHI of 56,075 individuals. Of the 1,337 unique advices, 838 records were accessed without authentication, by a web crawler only. The other 499 records, representing 40,360 individual members, were accessed by an unauthenticated user other than, or in addition to, a web crawler.

17. The investigation revealed that 28 records were accessed by personnel employed by DXC or the state of Indiana when investigating the incident. Therefore, 471 records, representing 39,984 individual members, were accessed by an unauthorized user, who was not a webcrawler or an employee of DXC or the state of Indiana. DXC was not able to identify who accessed those 471 records containing ePHI of about 39,984 individuals.

18. On or about May 10, 2017, DXC closed the Portal and commenced the investigation and repair of the vulnerability.

19. On or about May 10, 2017, FSSA notified the Office of the Indiana Attorney General (“OAG”) of the incident.

20. On or about June 23, 2017, DXC notified affected Indiana residents by mail.

**V. FIRST CLAIM FOR RELIEF:
UNAUTHORIZED USE OR DISCLOSURE OF PHI**

21. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

22. As a business associate of FSSA, DXC created or received PHI, including ePHI as defined by 45 C.F.R. § 160.103.

23. As a business associate of a covered entity, DXC was prohibited from using or disclosing PHI except as permitted or required by its business associate contract or other arrangement pursuant to 45 C.F.R. § 164.504(e) or as required by law. 45 C.F.R. § 164.502.

24. Disclosure means “the release, transfer, provision or access to, or divulging in any manner of information outside the entity holding the information.” 45 C.F.R. § 160.103.

25. Subjecting the ePHI of 56,075 individuals to possible access by unauthorized persons was a disclosure as defined by 45 C.F.R. § 160.103.

26. The disclosure did not fall within any exception under the Security Rule. 45 C.F.R. § 164.512.

27. By subjecting the PHI of 56,075 individuals to unauthorized access for approximately 40 days, DXC committed many violations of 45 C.F.R. § 164.502.

**VI. SECOND CLAIM FOR RELIEF:
FAILURE TO ENSURE CONFIDENTIALITY**

28. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

29. As a business associate, DXC was required to ensure the confidentiality, integrity, and availability of all ePHI that it or the FSSA created, received, maintained or transmitted. 45 C.F.R. § 164.306(a)(1).

30. “Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.” 45 C.F.R. § 164.304.

31. DXC’s failure to ensure the confidentiality of the ePHI of 56,075 individuals for about 40 days constituted many violations of 45 C.F.R. § 164.306(a)(1).

**VII. THIRD CLAIM FOR RELIEF:
FAILURE TO PROTECT SECURITY AND INTEGRITY OF PHI**

32. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

33. Business associates must shield ePHI against any reasonably anticipated threats or hazards to the security or integrity of the information. 45 C.F.R. § 164.306(a)(2).

34. DXC failed to shield ePHI from the “reasonably anticipated threat or hazard to the security or integrity” of the Portal and its vulnerabilities.

35. DXC’s failure to shield the ePHI of 56,075 individual for 40 days constituted many violations of 45 C.F.R. § 164.306(a)(2).

**VIII. FOURTH CLAIM FOR RELIEF:
FAILURE TO IMPLEMENT SUFFICIENT SECURITY MEASURES**

36. Plaintiff incorporates herein by reference all preceding paragraphs as if fully set forth herein.

37. Business Associates are required to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level compliant with 45 C.F.R. § 164.306(a). 45 C.F.R. § 164.308(a)(1)(ii)(A).

38. By allowing a vulnerability in the Portal to expose ePHI, DXC failed to implement security measures sufficient to comply with 45 C.F.R. § 164.306(a).

39. DXC's failure to implement security measures sufficient to prevent the exposure of ePHI of 56,075 individuals for 40 days constituted many violations of 45 C.F.R. 164.308(a)(1)(ii)(A).

IX. DEMAND FOR RELIEF

WHEREFORE, Plaintiff requests this Court to enter judgment against the Defendant, DXC Technology Services, LLC, for the following:

- a. An injunction against future violations of 45 C.F.R. 164.302, *et seq.*, pursuant to 42 U.S.C. 1320d-5(d)(1)(A);
- b. Statutory damages, pursuant to 42 U.S.C. 1320d-5(d)(2), in the amount of \$100,000;
- c. Costs of the action and reasonable attorney fees, pursuant to 42 U.S.C. 1320d-5(d)(3); and
- d. All other just and proper relief.

Respectfully submitted,

PLAINTIFF, STATE OF INDIANA *ex rel.*
Attorney General of Indiana

By: /s/Douglas S. Swetnam
Douglas S. Swetnam, Atty. No. 15860-49
Deputy Attorney General
Counsel for Plaintiff

Office of the Attorney General
302 West Washington Street
IGCS - 5th Floor
Indianapolis, IN 46204
Tel: (317) 232-6294 | Fax: (317) 232-7979
Email: dswetnam@atg.in.gov

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
Indianapolis Division**

STATE OF INDIANA, <i>ex rel.</i>)	
ATTORNEY GENERAL OF INDIANA,)	
)	
Plaintiff,)	CIVIL ACTION NO. 1:20-cv-1616
)	
v.)	
)	
DXC TECHNOLOGY SERVICES, LLC,)	
)	
Defendant.)	

CONSENT DECREE

The Plaintiff, State of Indiana, by and through its Attorney General as *parens patriae* for the residents of the State of Indiana (“the State”), by counsel, Douglas S. Swetnam, Deputy Attorney General, having filed a Complaint (“Complaint”), and Defendant, DXC Technology Services, LLC (“DXC”), a Virginia limited liability company, hereby enter into this Consent Decree without trial or adjudication of any issue of fact or law.

The parties believe it is in their best interests to resolve the issues presented by the State’s Complaint and avoid further litigation. The Consent Decree does not constitute an admission by DXC of any violation of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act OF 2009, and Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively referred to as “HIPAA”), or violation of any applicable law, nor shall it be construed as an abandonment by the State of its assertion that DXC violated those statutes. The parties consent to

entry of a final judgment in this proceeding by the Court and accept this Consent Decree as a final determination of the issues resolved herein.

I. JURISDICTION AND SCOPE OF JUDGMENT

1. It is this Court’s view that it has jurisdiction and venue over the subject matter of this action and the parties hereto.

2. The State asserts a cause of action pursuant to HIPAA.

3. DXC is a Virginia limited liability company with a principal office at 1775 Tysons Blvd., 9th Floor, Tysons Corner, Virginia 22102.

4. This Consent Decree constitutes a complete settlement and release by the State of all civil claims that could have brought against DXC in relation to violations of HIPAA, in connection with the alleged exposure of protected health information (“PHI”) described in the Complaint.

Now, therefore, by consent and agreement of the parties, it is **ORDERED, ADJUDGED, AND DECREED** as follows:

II. RELIEF

5. Any term used in this Consent Decree that is defined by 45 C.F.R. § 160.103 shall have the meaning provided therein, except that, for purposes of this Consent Decree, the term “PHI” shall be limited to PHI created, received, maintained, or transmitted by DXC on behalf of the Indiana Family and Social Services Administration (“FSSA”) and the term “ePHI” shall be limited to ePHI created, received, maintained, or transmitted by DXC on behalf of the FSSA.

6. The Effective Date of this Consent Decree shall be the date on which it is approved by this Court.

7. Pursuant to 42 U.S.C. § 1320d-5(d)(1), DXC is hereby enjoined from committing acts and practices in violations of HIPAA, specifically:

- a. Using or disclosing PHI other than as permitted or required by its business associate contract or other arrangement pursuant to 45 C.F.R. § 164.504(e), or as required by law, in violation of 45 C.F.R. § 164.502;
- b. Failing to ensure the confidentiality, integrity, and availability of all ePHI in violation of 45 C.F.R. § 164.306(a)(1);
- c. Failing to shield ePHI against reasonably anticipated threats or hazards to the security or integrity of the information, in violation of 45 C.F.R. § 164.306(a)(2);
and
- d. Failing to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(a), in violation of 45 C.F.R. 164.308(a)(1)(ii)(A).

8. The obligations set forth in paragraph 7 shall expire at the conclusion of a three (3) year period after the Effective Date of this Consent Decree. Nothing in this paragraph should be construed or applied to excuse DXC from its obligation to comply with all applicable state and federal laws, regulations, and rules.

9. Within ninety (90) days of the Effective Date of this Consent Decree, DXC shall provide to the Indiana Attorney General a copy of its policies and procedures that address DXC's safeguarding of PHI, namely its *Electronic Protected Health Information Security Policy*, and shall send the policy by mail or email to the attention of:

Douglas S. Swetnam, Section Chief
Data Privacy and Identity Theft
Unit Office of the Attorney General
302 W. Washington St.
Indiana Government Center South – 5th Floor
Indianapolis, Indiana, 46204
Douglas.Swetnam@atg.in.gov
Tel: 317-232-6294

10. Within thirty (30) days of the Effective Date of this Consent Decree, DXC shall pay \$55,000 to the Indiana Attorney General. Payment shall be in the form of a money order, cashier's check, wire transfer, or otherwise as agreed by the parties and made payable to the State of Indiana.

11. This Consent Decree is binding upon DXC, including any agents, employees, successors, and assigns of all or substantially all of the assets of its business.

12. The State shall use said payment for any purpose allowable under state law, including to protect the privacy and security of Indiana residents' personal information.

13. This Consent Decree contains the entire agreement and understanding of the parties with respect to the matters addressed herein.

14. Nothing in this Consent Decree shall be construed to affect or deprive any private right of action that any consumer, person, entity, or any local, state, federal, or other governmental entity may hold against DXC, except as otherwise provided by law.

15. If any clause, provision, or section of this Consent Decree shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, section of this Consent Decree and this Consent Decree shall be construed and enforced as if such clause, provision, or section had not been contained herein.

16. Nothing in this Consent Decree shall be construed or applied to excuse DXC from its obligations to comply with all applicable Indiana statutes and other laws.

17. Any failure by any party to this Consent Decree to insist upon the strict performance by the other party of any of the provisions of this Consent Decree shall not be deemed a waiver of any of the provisions of this Consent Decree, and such party, notwithstanding such failure, shall have the right thereafter to insist upon the specific performance of any and all of the provisions of this Consent Decree and the imposition of any applicable penalties, including but not limited to contempt, civil penalties, and/or the payment of attorney fees.

18. Time shall be of the essence with respect to each provision of this Consent Decree that requires action to be taken by DXC within a stated time period.

19. This Consent Decree may be executed in any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart hereof and all of which together shall constitute one and the same document. One or more counterparts of this document may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

III. CONTINUING JURISDICTION

20. The Court shall retain jurisdiction for the purpose of issuing such orders as may be necessary to interpret or enforce the provisions herein.

[Signature pages follow]

IN WITNESS WHEREOF, the parties have executed this Consent Decree:

FOR PLAINTIFF, STATE OF INDIANA ex rel.
ATTORNEY GENERAL OF INDIANA

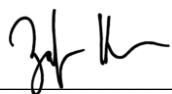
By:

/s/ Douglas S. Swetnam
Douglas S. Swetnam, Atty. No. 15860-49
Deputy Attorney General
Counsel for Plaintiff

Office of the Attorney General
Indiana Government Center South, Fifth Floor
302 West Washington Street
Indianapolis, Indiana 46204
Phone: (317) 232-6294
Email: dswetnam@atg.in.gov

Date: June 12, 2020

FOR DEFENDANT, DXC TECHNOLOGY SERVICES, LLC



Signature

Zafar Hasan

Name

VP, Chief Corporate Counsel & Asst. Secretary
Title

June 10, 2020

Date: