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