

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

WESTEND DENTAL LLC, ARLINGTON
WESTEND DENTAL LLC, SHERMAN
WESTEND DENTAL LLC, FOUNTAIN
SQUARE WESTEND DENTAL LLC,
LAFAYETTE WESTEND DENTAL LLC,
and AFFORDABLE WESTEND DENTAL
LLC,

Defendants.

CASE NO.

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 Attorneys General Douglas S. Swetnam and Jennifer M. Van Dame, and Defendants, Westend Dental LLC, Arlington Westend Dental LLC, Sherman Westend Dental LLC, Fountain Square Westend Dental LLC, Lafayette Westend Dental LLC, and Affordable Westend Dental LLC (together, “Westend Dental”) (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 State’s investigation of Westend Dental’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 Westend Dental of any violation of the Relevant Laws, nor shall it be construed as an abandonment by the State of its allegations that Westend Dental 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. Westend Dental is a series of Indiana-based limited liability companies operating seven (7) dental offices at the following Indiana addresses:

- a. Westend Dental LLC, 3611 W 16th St., Indianapolis, IN 46222;
- b. Arlington Westend Dental LLC, 5900 E 10th St., Indianapolis, IN 46219;

- c. Sherman Westend Dental LLC, 3636 E 38th St., Indianapolis, IN 46218;
- d. Fountain Square Westend Dental LLC, 1535 Prospect St., Indianapolis, IN 46203;
- e. Lafayette Westend Dental LLC, 311 Sagamore Pkwy N. STE 2, Lafayette, IN 47904; and
- f. Affordable Westend Dental LLC, 2915 Lafayette Road, Indianapolis, IN 46222.

BACKGROUND

3. On or around October 20, 2020, Westend Dental experienced a ransomware attack that exposed the Personal Information and/or Protected Health Information of Indiana residents (the “October 2020 Data Breach”).

4. The OAG investigated the October 2020 Data Breach pursuant to the Relevant Laws.

5. The OAG’s investigation of the October 2020 Data Breach prompted the OAG to investigate Westend Dental’s compliance with HIPAA generally.

STIPULATIONS

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

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

8. At all times relevant to this matter, Westend Dental was engaged in trade and commerce affecting consumers in the State of Indiana insofar as Westend Dental provides dental products and services to consumers in Indiana. Westend Dental was also in possession of the Personal Information and Protected Health Information of Indiana residents.

9. The injunctive terms contained in this Consent Judgment are entered pursuant to 42 U.S.C. § 1320d-5(d)(1)(A) and Ind. Code §§ 24-5-0.5-4(c), 24-4.9-4-2, and 24-4.9-3-3.5(f).

10. 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

11. 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.

12. 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

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

13. "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 ePHI and to manage the conduct of the Covered Entity's or Business Associate's workforce in relation to the protection of that information.

14. "Breach" shall be defined in accordance with 45 C.F.R. § 164.402 and means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

15. "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 PHI.

16. "Consumer" and "Consumers" shall mean any individuals whose PI and/or ePHI is collected, maintained, processed, stored, transmitted, or otherwise accessible on the Westend Dental Network.

17. “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.

18. “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.

19. “Delete” or “Deleted” means to remove information or data such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

20. “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.

21. “Effective Date” shall mean the date on which this Consent Judgment is approved by the Court.

22. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.

23. “Encrypt”, “Encrypted” or “Encryption” shall mean encoding data into ciphertext—at rest or in transit—rendering it unusable, unreadable, or indecipherable without converting the ciphertext to plaintext, through the use of a

confidential process and key leveraging a security technology, methodology, or encryption algorithm commensurate with the sensitivity of the data at issue.

24. "Governance Process" shall mean any written policy, standard, procedure, or process (or any combination thereof) designed to achieve a control objective.

25. "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.

26. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule that, when using or disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit PHI 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).

27. "Patient Authorization" shall be written and shall comply with and satisfy the requirements of 45 C.F.R. § 164.508. Patient Authorizations shall be written in plain language and shall contain the signature of the individual authorizing the use or disclosure of his or her PHI and the date, and if signed by a personal representative of the individual, a description of such representative's

authority to act for the individual.

28. “Personal Information” or “PI” shall be defined in accordance with the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9-2-10.

29. “Physical Safeguards” shall be defined in accordance with 45 C.F.R. § 164.304 and means physical measures, policies, and procedures to protect a Covered Entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

30. “Privacy Rule” shall refer to the HIPAA regulations that establish national standards to safeguard individuals’ medical records and other PHI, 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.

31. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103

32. “Security Incident” shall be defined in accordance with 45 C.F.R. § 164.304 and means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

33. “Security Rule” shall refer to the HIPAA regulations that establish national standards to safeguard individuals’ 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 C.

34. “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 ePHI and control access to it.

35. “Westend Dental Network” shall mean all networking equipment, systems, databases or data stores, applications, servers, and endpoints that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned, operated, and/or controlled by Westend Dental; and (c) collect, maintain, process, store, transmit, or have access to PI and/or ePHI of Consumers.

INJUNCTIVE PROVISIONS

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

COMPLIANCE WITH LAW

36. **HIPAA:** Westend Dental shall comply with the Privacy Rule and Security Rule and shall implement all Administrative Safeguards, Physical Safeguards, and Technical Safeguards required by HIPAA.

37. **DSBA and DCSA:** Westend Dental shall comply with DSBA and DCSA in connection with its collection, maintenance, and safeguarding of PI, PHI, and ePHI.

38. **Prohibited Misrepresentations and Omissions:** Westend Dental shall not misrepresent or omit information capable of misleading Consumers

regarding the extent to which Westend Dental maintains and/or protects the privacy, security, confidentiality, or integrity of PI, PHI, or ePHI.

39. **Breach Notification:** Westend Dental shall comply with the breach notification requirements of HIPAA and DSBA.

40. **Notice of Privacy Practices:** Westend Dental shall maintain and provide patients with a notice of privacy practices in accordance with 45 C.F.R. § 164.520. Westend Dental's notice of privacy practices shall include the information required by 45 C.F.R. § 164.520(b). The notice of privacy practices required by this paragraph shall be prominently posted and made available on the Westend Dental website.

INCIDENT AND BREACH RESPONSE AND NOTIFICATION

41. **Investigation and Response to Security Incidents:** Westend Dental shall comply with 45 C.F.R. § 164.308(a)(6) and implement policies and procedures to address Security Incidents. Westend Dental shall identify and promptly respond to suspected or known Security Incidents and mitigate, to the extent practicable, harmful effects of Security Incidents. Westend Dental shall promptly investigate Security Incidents and maintain documentation sufficient to show the investigative and responsive actions taken in connection with each Security Incident and the determination as to (a) whether and how a Breach occurred, and (b) whether notification under HIPAA and/or the DSBA is required ("Security Incident Reports"). Westend Dental shall produce any Security Incident Report to the OAG upon request.

42. **Timely Breach Notification:** In the case that breach notification under HIPAA and/or the DSBA is required, Westend Dental shall provide timely notification to Consumers as required by law. The deadline for timely notification to Consumers shall be calculated from the first day on which such Breach is known to Westend Dental, or would have been known to Westend Dental through reasonable diligence, not when the investigation of such Breach is complete.

43. **Incident Response Plan:** Westend Dental shall implement and maintain a written plan to prepare for and respond to Security Incidents and Breaches (“Incident Response Plan”). Westend Dental shall revise and update the Incident Response Plan, as necessary, including to adapt to any changes to the Westend Dental Network. Such a plan shall, at a minimum, identify and describe the following phases:

- a. Preparation;
- b. Detection and Analysis;
- c. Containment;
- d. Law Enforcement Notification and Coordination;
- e. Eradication;
- f. Recovery;
- g. Consumer and Regulator Notification, as applicable; and
- h. Post-Incident Analysis and Remediation.

44. **Table-Top Exercises:** Westend Dental shall conduct Incident Response Plan exercises (“Table-Top Exercises”), at a minimum once per year, to test and assess its preparedness to respond to Security Incidents and Breaches.

NOTIFICATION OF OCTOBER 2020 DATA BREACH

45. **Individual Notification:** Within sixty (60) days after the Effective Date, Westend Dental shall individually notify all individuals who were patients of Westend Dental as of November 20, 2023, of the October 2020 Data Breach. The notification required by this paragraph shall be a written notification by first-class mail and shall comply with the “content of notification” requirements of 45 C.F.R. § 164.404(c).

46. **Media Notification:** Within thirty (30) days after the Effective Date, Westend Dental shall notify prominent media outlets serving the State in accordance with 45 C.F.R. § 164.406. The notification required by this paragraph shall comply with the “content of notification” requirements of 45 C.F.R. §§ 164.406(c) & 164.404(c).

47. **Website Notice:** Beginning within thirty (30) days after the Effective Date and for a period of one hundred and eighty (180) days, Westend Dental shall provide notice of the October 2020 Data Breach in the form of a conspicuous posting on the home page of the Westend Dental website (<https://www.mywestenddental.com/>). The notice required by this paragraph shall comply with the “content of notification” requirements of 45 C.F.R. § 164.404(c) and shall include a phone number that Westend Dental patients can call to obtain additional information regarding the October 2020 Data Breach.

INFORMATION SECURITY PROGRAM

48. **Information Security Program:** Within ninety (90) days after the Effective Date, Westend Dental shall implement, maintain, regularly review and

revise, and comply with a comprehensive information security program (“Information Security Program”), the purpose of which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of ePHI and PI on the Westend Dental Network, consistent with the Relevant Laws. The Information Security Program shall be documented in Governance Processes and shall contain administrative, technical, and physical safeguards appropriate to:

- a. The size and complexity of Westend Dental’s operations;
- b. The nature and scope of Westend Dental’s activities; and
- c. The sensitivity of the ePHI and PI stored within, accessed, or transmitted through the Westend Dental Network.

The Information Security Program required by this Consent Judgment shall include at least the requirements of Paragraphs 49 through 71 in this Consent Judgment.

49. HIPAA Risk Analysis and Risk Management Plan: Westend Dental shall conduct accurate and thorough annual assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Westend Dental, and implement security measures sufficient to reduce the risks and vulnerabilities identified by such assessments to a reasonable and appropriate level in accordance with 45 C.F.R. § 164.308(a)(1)(ii)(A)-(B). Westend Dental shall document the risk analyses and risk management plans required by this paragraph and shall produce such documentation to the OAG upon request.

50. Oversight of Third-Party Vendors: Westend Dental shall oversee its third-party vendors who have access to the Westend Dental Network, or who hold or

store ePHI and/or PI on Westend Dental's behalf, by maintaining and periodically reviewing and revising, as needed, a Governance Process for assessing vendor compliance with Westend Dental's Information Security Program including whether the vendor's security safeguards are appropriate for that business.

51. **Governance:** Westend Dental shall designate an individual who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter referred to as the "Security Officer"). The Security Officer shall be independent (*i.e.* not a family member of any owner, executive, officer, manager, or supervisor of any Westend Dental entity); shall have appropriate training, expertise, and experience to oversee the Information Security Program; and shall regularly report on the status of the Information Security Program, the security risks faced by Westend Dental, resources required for implementation of the Information Security Program, and the security implications of Westend Dental's business decisions.

52. **Necessary Resources and Support:** Westend Dental shall ensure that the Security Officer, Information Security Program, and corresponding staff receive the resources and support reasonably necessary to ensure that the Information Security Program functions as required by this Consent Judgment.

TRAINING REQUIREMENTS

53. **Training:**

- a. Employees and contractors who are responsible for implementing, maintaining, or monitoring the Information Security Program shall

receive specialized training to help effectuate Westend Dental's compliance with the terms of this Consent Judgment. Westend Dental shall provide the training required by this paragraph to all such employees within thirty (30) days of the Effective Date of this Consent Judgment or prior to an employee starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program. Westend Dental shall document the trainings, including the date(s) upon which they were provided and to whom.

- b. Employees and contractors who handle PI, PHI and/or ePHI shall receive training on safeguarding and protecting PI, PHI, and ePHI. Such training shall be appropriate to employees' and contractors' responsibilities and functions and shall occur on an annual basis, or more frequently if appropriate, beginning within thirty (30) days of the Effective Date of this Consent Judgment or prior to an employee or contractor handling PI, PHI, and/or ePHI. Westend Dental shall document the trainings, including the date(s) upon which they were provided and to whom.

**PERSONAL AND PROTECTED HEALTH
INFORMATION SAFEGUARDS**

54. **Data Minimization:** Westend Dental shall implement, maintain, regularly review and revise as necessary, and comply with a Governance Process establishing that PI will be collected, processed, and stored to the minimum extent

necessary to accomplish the intended legitimate business purpose(s) in using such information.

55. **Minimum Necessary Standard:** Westend Dental shall comply with the Minimum Necessary Standard and shall implement, regularly review and revise as necessary, and maintain a Governance Process requiring Westend Dental to make reasonable efforts, when using or disclosing PHI or ePHI, to limit the use or disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

56. **Business Associate Contracts:** Westend Dental shall execute business associate contracts in accordance with 45 C.F.R. §§ 164.502(e) & 164.504(e). Prior to any disclosure of PHI or ePHI to a Business Associate, Westend Dental shall execute a business associate contract with the Business Associate that complies with 45 C.F.R. § 164.504(e)(2). Westend Dental's business associate contracts shall be written, dated, and produced to the OAG upon request.

57. **Email Accounts and Other Platforms and Services:** Westend Dental shall not use any non-HIPAA-compliant email services or other digital platforms or services that do not comply with HIPAA to conduct business or otherwise store, transmit, or receive ePHI. Within ninety (90) days of the Effective Date, all ePHI of Consumers stored or accessible in any non-HIPAA-compliant email account or other non-HIPAA-compliant digital platform or service shall be located and Deleted.

58. **Social Media and Online Reviews:** Westend Dental shall not disclose PHI on social media websites, in response to online reviews, in any advertisements or promotions, or on any other website or digital platform or service without Patient Authorization. Westend Dental shall implement and maintain written policies and procedures for social media, online reviews, and other advertisements or promotions that are designed to ensure compliance with the Relevant Laws. Within thirty (30) days of the Effective Date, all social media posts and responses to online reviews that have disclosed PHI without Patient Authorization shall be Deleted.

SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

59. **Network Segmentation:** Westend Dental shall implement and maintain network segmentation policies and procedures designed to properly segment the Westend Dental Network.

60. **Penetration Testing:** Westend Dental shall complete penetration testing designed to identify, assess, and remediate potential security vulnerabilities. Penetration testing shall occur regularly and be documented. Westend Dental shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation.

61. **Access Control and Account Management:**

- a. Westend Dental shall implement and maintain appropriate controls to manage access to, and use of, all Westend Dental Network accounts with access to PI or ePHI, including, without limitation, individual accounts,

administrator accounts, service accounts, and vendor accounts.

- b. Westend Dental shall implement and maintain policies and procedures to ensure that access to PI and ePHI is granted only after a user has been properly identified and authenticated and under the principle of least privilege.
- c. Westend Dental shall require multi-factor authentication or equivalent enhanced authentication measures for remote access to the Westend Dental Network.
- d. Westend Dental shall implement and maintain policies and procedures to regularly review and audit accounts, permissions, and access levels of users, and to promptly remove accounts, permissions, and access when such accounts, permissions, or access are no longer necessary or appropriate.
- e. Westend Dental shall not permit use of shared accounts with access to PI or ePHI.
- f. Westend Dental shall regularly review records of information system activity, such as audit logs and access reports, in accordance with 45 C.F.R. § 164.308(a)(1)(ii)(D).

62. **Password Management:** To the extent that Westend Dental maintains accounts requiring passwords, Westend Dental shall implement and maintain password policies and procedures requiring appropriate password

complexity, change intervals, and secure storage of passwords. Westend Dental shall not store passwords in plaintext.

63. **Unauthorized or Malicious Applications:** Westend Dental shall implement maintain controls designed to detect and protect against the execution or installation of unauthorized or malicious applications on the Westend Dental Network.

64. **Logging and Monitoring:** Westend Dental shall implement and maintain controls to centralize logging and monitoring of the Westend Dental Network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks are appropriately monitored and tested to ensure proper configuration and maintenance. Westend Dental 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 Security Incidents and Breaches.

65. **Change Control:** Westend Dental shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to manage and document changes to the Westend Dental Network.

66. **Asset Inventory:** Westend Dental shall utilize processes and, where practicable, automated tool(s) to regularly inventory and classify all assets that comprise the Westend Dental Network. For purposes of this paragraph, "assets" shall

include networking equipment, databases or data stores, applications, servers, devices, endpoints, and other systems within the Westend Dental Network.

67. Intrusion Detection and Prevention: Westend Dental shall implement and maintain intrusion detection and prevention systems, endpoint protection systems, threat monitoring systems, and similar technologies reasonably designed to detect and prevent malicious activity and unauthorized access to the Westend Dental Network.

68. Vulnerability Management: Westend Dental shall conduct regular vulnerability scanning using industry-standard tools and shall take appropriate steps to promptly remediate identified vulnerabilities.

69. Security Updates and Patch Management: Westend Dental shall implement and maintain processes and procedures for security updates and patch management to maintain, keep updated, and support the software on the Westend Dental Network, taking into consideration the impact a software update will have on data security in the context of the Westend Dental Network and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. Such processes and procedures shall include a schedule to install security updates and patches in a timely manner that considers (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the vulnerability in the context of the Westend Dental Network, the impact on Westend Dental's ongoing business and network

operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by a U.S. government authority.

70. **Encryption:** Westend Dental shall Encrypt PI and ePHI in transit and at rest.

71. **Data Backup Plan:** Westend Dental shall establish and implement procedures to create and maintain retrievable exact copies of ePHI in accordance with 45 C.F.R. § 164.308(a)(7)(ii)(A). Westend Dental shall oversee any third-party vendors who create backups on Westend Dental's behalf to ensure that backups are created in accordance with the procedures required by this paragraph.

ASSESSMENT AND REPORTING REQUIREMENTS

72. **Third-Party Assessment of HIPAA Compliance:** Within thirty (30) days of the Effective Date, Westend Dental shall engage an independent third party ("Third-Party HIPAA Assessor") to conduct an assessment of Westend Dental's compliance with the Privacy Rule and the Security Rule ("Third-Party HIPAA Assessment"). The Third-Party HIPAA Assessor have at least five (5) years of experience evaluating HIPAA compliance. Westend Dental shall disclose all material facts to the Third-Party HIPAA Assessor and not misrepresent in any manner, expressly or by implication, any fact material to the Third-Party HIPAA Assessor's determinations and assessments. The Third-Party HIPAA Assessor shall document the Third-Party HIPAA Assessment, including the Third-Party HIPAA Assessor's findings and recommendations, in a written report, a copy of which shall be produced to the OAG upon request. Westend Dental shall review and, to the extent necessary,

promptly revise its current practices, policies, and procedures based on the findings and recommendations of the Third-Party HIPAA Assessment.

73. **Third-Party Assessments of Information Security Program:** For a period of seven (7) years, Westend Dental shall engage an independent third party (“Third-Party Security Assessor”) to conduct biennial assessments of its information security practices, as well as its compliance with the terms of this Consent Judgment (“Third-Party Security Assessments”).

- a. The Third-Party Security Assessor shall be a Certified Information Systems Security Professional (CISSP) or a Certified Information Systems Auditor (CISA), or a similarly qualified person or organization and have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security.
- b. The reporting period for the Third-Party Security Assessments shall cover: (1) the first one hundred and eighty (180) days after the Effective Date for the initial Third-Party Security Assessment; and (2) every other year thereafter for seven (7) years, for a total of four (4) Third-Party Security Assessments completed in the first, third, fifth, and seventh years after the Effective Date.
- c. The Third-Party Security Assessments shall:
 - i. Follow a NIST Cybersecurity Framework or another established industry standard cybersecurity framework;

- ii. Identify the specific administrative, technical, and physical safeguards maintained by Westend Dental's Information Security Program;
 - iii. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering Westend Dental's size and complexity, the nature and scope of Westend Dental's activities, and the sensitivity of the PI and ePHI maintained on the Westend Dental Network;
 - iv. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Westend Dental meet the requirements of the Information Security Program; and
 - v. Identify specific evidence (including, but not limited to, documents reviewed and interviews conducted) examined to make such determinations and assessments.
- d. Westend Dental shall disclose all material facts to the Third-Party Security Assessor and not misrepresent in any manner, expressly or by implication, any fact material to the Third-Party Security Assessor's determinations and assessments.
- e. The Third-Party Security Assessor shall document each Third-Party Security Assessment, including the Third-Party Security Assessor's findings and recommendations, in a written report ("Third-Party

Security Assessment Report”), a copy of which shall be produced to the OAG within thirty days (30) of completion of the Third-Party Security Assessment.

- f. Within ninety (90) days of Westend Dental’s receipt of each Third-Party Security Assessment Report, Westend Dental shall review and, to the extent necessary, revise its current policies and procedures based on the findings and recommendations of the Third-Party Security Assessment Report. Within one hundred eighty (180) days of Westend Dental’s receipt of each Third-Party Security Assessment Report, Westend Dental shall produce to the OAG a written description of any action taken and, if no action is taken, a written description of why no action is necessary, in response to each Third-Party Security Assessment Report.

DOCUMENT RETENTION

74. Westend Dental shall retain and maintain the documentation required by the foregoing paragraphs for a period of no less than seven (7) years.

PAYMENT TO THE STATE

75. Westend Dental shall pay a total of **Three Hundred and Fifty Thousand Dollars (\$350,000.00)** to the Office of the Indiana Attorney General, to be used for any purpose allowable under Indiana law. Westend Dental shall comply with the following payment schedule:

- a. Within thirty (30) days of the Effective Date, Westend Dental shall pay One Hundred Thousand Dollars (\$100,000.00);
- b. By April 30, 2025, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Seven Cents (\$41,666.67);
- c. By October 15, 2025, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Seven Cents (\$41,666.67);
- d. By April 30, 2026, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Seven Cents (\$41,666.67);
- e. By October 15, 2026, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Seven Cents (\$41,666.67);
- f. By April 30, 2027, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Six Cents (\$41,666.66); and
- g. By October 15, 2027, Westend Dental shall pay Forty-One Thousand Six Hundred Sixty-Six Dollars and Sixty-Six Cents (\$41,666.66).

Payment in seven (7) installments is expressly premised upon the truthfulness and accuracy of Westend Dental's representations of its inability to pay the amount in its entirety within thirty (30) days of the Effective Date. 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, Westend Dental shall provide the State with an IRS Form W-9 upon execution of this Consent Judgment.

RELEASE

76. Following full payment of the amount due under this Consent

Judgment, the State shall release and discharge Westend Dental from all civil claims that the State could have brought under the Relevant Laws based on Westend Dental'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 Westend Dental has under this Consent Judgment. Further, nothing in this Consent Judgment shall be construed to (a) create, waive, or limit any private right of action; or (b) excuse or exempt Westend Dental from complying with any state or federal law, rule, or regulation in the future.

77. Notwithstanding any term of this Consent Judgment, any and all of the following forms of liability are specifically excluded from the release in Paragraph 76 above as to any entity or person, including Westend Dental:

- a. Any criminal liability that any person or entity, including Westend Dental, has or may have; and
- b. Any civil liability or administrative liability that any person or entity, including Westend Dental, has or may have under any statute, regulation, or rule not expressly covered by the release in Paragraph 76 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.

GENERAL PROVISIONS

78. Westend Dental represents that it has fully read this Consent Judgment

and understands the legal consequences attendant to entering into this Consent Judgment. Westend Dental 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 Westend Dental, Westend Dental agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Consent Judgment against Westend Dental.

79. Nothing in this Consent Judgment shall be construed to limit the authority or ability of the Indiana Attorney General to protect the interests of the State of Indiana or the people of Indiana. This Consent Judgment shall not bar the OAG or any other governmental entity from enforcing laws, regulations, or rules against Westend Dental for conduct subsequent to or otherwise not covered by this Consent Judgment.

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

81. Any failure of the State to exercise any of its rights under this Consent

Judgment shall not constitute a waiver of any rights hereunder.

82. The duties, responsibilities, burdens, and obligations undertaken in connection with this Consent Judgment shall apply to Westend Dental and its owners, executives, officers, and employees.

83. Westend Dental shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Consent Judgment or for any other purpose that would otherwise circumvent any term of this Consent Judgment. Westend Dental shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Consent Judgment.

84. Westend Dental agrees that this Consent Judgment does not entitle it to seek or to obtain attorneys' fees under any statute, regulation, or rule, and Westend Dental further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

85. If any portion of this Consent Judgment is held invalid or unenforceable, the remaining terms of this Consent Judgment shall not be affected and shall remain in full force and effect.

86. Westend Dental waives 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 court order. However, the Parties may agree in writing, through counsel, to an extension of any time period specified in this Consent Judgment without a court order.

87. The Parties hereby acknowledge that their undersigned representative or representatives are authorized to enter into and execute this Consent Judgment. Westend Dental 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.

88. 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.

NOTICES

89. 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. Any notices or other documents sent pursuant to the Consent Judgment shall be sent to:

a. For the State:

Jennifer M. Van Dame
Assistant Section Chief – Data Privacy & Identity Theft Unit

Consumer Protection Division
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
jennifer.vandame@atg.in.gov

and

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

b. For Defendants:

Deept Rana
3611 W. 16th Street
Indianapolis, IN 46222
deept@mywestenddental.com

and


Brian S. Jones
Bose McKinney & Evans LLP
111 Monument Circle, Ste. 2700
Indianapolis, IN 46204
b.jones@boselaw.com

A Party may update its designee or address by sending written notice to the other Party informing them of the change.

IT IS STIPULATED:

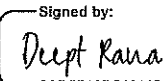
FOR THE STATE OF INDIANA

Office of Indiana Attorney General

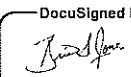
By 
Jennifer M. Van Dame
Attorney No. 32788-53
Deputy Attorney General

Date: 12-19-2024

FOR DEFENDANTS

By 
Deept Rana
Clinical Director
Westend Dental

Date: 12/19/2024 | 3:36 PM EST

By 
Brian S. Jones
Atty No. 29578-49
Bose McKinney & Evans LLP
111 Monument Circle, Ste. 2700
Indianapolis, IN 46204

Date: 12/19/2024 | 3:58 PM EST

SO ORDERED, ADJUDGED, AND DECREED:

By _____
JUDGE

Date: _____