

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 2026- 057

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

BOSTON CHILDREN’S HEALTH PHYSICIANS, LLP,

and

XTIUM,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“OAG”) commenced an investigation pursuant to Executive Law § 63(12), General Business Law (“GBL”) § 899-bb, 45 C.F.R. Part 160, and 45 C.F.R. Part 164 Subparts A and C, into data security incidents at Boston Children’s Health Physicians, LLP (“BCHP”) and XTIUM (BCHP and XTIUM each individually a “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of OAG’s investigation and the relief agreed to by the OAG and each Respondent, whether acting through their respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively and separately, the “Parties”).¹

OAG FINDINGS

1. BCHP is a multi-site medical practice based in New York, providing comprehensive medical care for young patients.

¹ The investigation was conducted with the Connecticut Attorney General’s office who entered into a similar agreement with Respondents.

2. BCHP doctors practice in over 60 locations in New York and five in Connecticut. BCHP's network includes over 300 doctors.

3. BCHP is a "covered entity" under HIPAA, the Health Insurance Portability and Accountability Act of 1996. A covered entity under HIPAA must comply with certain rules and requirements to protect the privacy and security of certain protected health information and must provide individuals with certain rights with respect to their protected health information.

4. BCHP has limited in-house information technology ("IT") and information security resources. BCHP outsources many IT functions to third-party vendors. At the time of the fall 2024 BCHP data breach, there were only two BCHP employees responsible for overseeing the company's IT and information security functions.

5. BCHP utilized two different IT vendors at the time of the data breach. The first IT vendor was responsible for both management of and security for BCHP's company's **active patient records system**. This system was **not** breached in the fall 2024 BCHP data breach.

6. The second IT vendor was Axispoint Technology Solutions Group, Inc., which has since merged with Evolve IP to form XTium (collectively "XTium"). XTium was contractually responsible for the **management** of (**not** security for) BCHP's **other IT systems**. It was these other IT systems that were breached in the fall 2024 attack.

7. XTium is a contractual "business associate" of BCHP under HIPAA. A HIPAA business associate is an individual or entity that performs functions or services for a HIPAA-covered entity and has access to protected health information.

8. XTium contracted with BCHP to provide services under the category of a "managed service provider" or "MSP". MSPs provide general technology services, such as IT systems management. MSP services are administrative and operational in nature. MSP services

typically focus on system efficiency, usability, and performance. MSPs generally do **not** provide security services, such as threat detection, threat prevention, risk management, scanning, incident response, and compliance. In contrast, a “managed **security** service provider” or “MSSP” provides those types of security services to clients.

The August 2024 Incident

9. During August 2024, a threat actor infiltrated XTium. XTium later learned that the initial infiltration into its systems led to the infiltration of eighteen of its client systems. Of these eighteen clients, however, only BHP suffered a data breach as a result of the infiltration.

10. On September 6, 2024, XTium notified BHP that XTium had suffered a system breach. On September 7, 2024, BHP reset all BHP system **user** passwords but took no further action, such as resetting system passwords, resetting administrator passwords, or isolating the BHP system from the internet until it could confirm no breach had occurred.

11. On September 10, 2024, BHP detected unauthorized system activity and cut off internet access to the BHP network while it investigated. BHP was able to remediate its system and bring it back online by September 13, 2024.

12. A third party investigation discovered that the threat actors had accessed and exfiltrated an unencrypted archive of patient billing records, including patient and guarantor names, addresses, dates of birth, social security information, health insurance information, billing information, and treatment information. Employee records were also exfiltrated, containing name, address, date of birth, social security number, and driver’s license number.

13. The records of approximately 825,000 New Yorkers were exfiltrated by the threat actors. Over 170,000 of these records included New York resident social security numbers and/or driver’s license numbers.

14. BCHP notified individuals as required by federal and state law. BCHP also offered one year of free credit monitoring to affected individuals.

15. XTIUM also suffered a data breach as a result of the infiltration of its systems. Approximately 1,000 XTIUM employee records were exfiltrated, including the records of over 200 New Yorkers.

XTIUM Did Not Reasonably Safeguard the Private Information of New York Residents.

16. XTIUM failed to adopt reasonable safeguards to protect the private information of New Yorkers. This enabled threat actors to harvest the information of New Yorker's as outlined in paragraph 1-15 above.

17. XTIUM's system was accessed by the threat actors through its implementation of a third party remote support tool used to service clients, including BCHP. XTIUM did not implement the remote support tool utilizing all of the security measures recommended by the third party vendor.

18. XTIUM did not have sufficient logging or monitoring in place to protect, detect, and defend against misuse of the remote support tool account. XTIUM's logging and monitoring of its own sign-in processes were so deficient at the time of the attack that XTIUM cannot definitively confirm how the threat actors accessed the XTIUM system.

19. XTIUM did not reasonably safeguard BCHP's data while carrying out its responsibilities. For example, while BCHP failed to implement and enforce common standard security policies for its IT system, XTIUM neither requested these BCHP policies nor followed common standard practices when handling BCHP tasks for which BCHP provided no policies. As a result, XTIUM managed certain IT functions in the BCHP system using a single shared administrative account with unrestricted access and unlimited privileges. Regardless of BCHP lacking the necessary policies to govern such accounts, XTIUM should have applied common

standard practices to secure the client accounts it used. Moreover, XTium's monitoring and logging of its use of this administrative account was so poor that it prevented meaningful forensic analysis of the attack.

20. The threat actor also used their access to XTium's system to steal XTium employment records containing the personal information of approximately 1,000 employees, 200 of which are New York residents.

BCHP Did Not Reasonably Safeguard the Private Information of New York Residents.

21. BCHP failed to adopt reasonable safeguards to protect the private information of New Yorkers. This enabled threat actors to harvest the information of New Yorker's outlined in paragraph 1-15 above.

22. The threat actor that attacked XTium was able to infiltrate eighteen of XTium's client systems. Only the intrusion into BCHP's system resulted in a client data breach, however, because BCHP failed to reasonably safeguard its own systems.

23. After the attacker used the shared, unrestricted XTium administrative account to access BCHP's system, the threat actor compromised four additional unrestricted BCHP administrative accounts. These four accounts were "non-human service accounts" that should have been restricted in multiple ways, including barring interactive logins by humans. Because BCHP failed to adopt and enforce common standard information security policies, these accounts were used by threat actors to gain access to BCHP's entire system. The threat actors then used their access and exfiltrate the unencrypted archive of client information from an accessible server.

24. BCHP failed to design, implement, and enforce a reasonable information security program to protect the personal data it collected. In particular, BCHP's IT system did **not** reasonably utilize the following common information security policies and procedures:

- a. **account permission and restrictions** to set limits on each account to ensure only authorized accounts could perform certain tasks;
- b. **access segmentation** to divide the network into smaller, isolated sections to limit account access and contain threats;
- c. **principle of least privilege** to only grant accounts and systems the minimum level of access and activity permissions necessary to perform their tasks;
- d. **access control** to authorize and analyze account access events to objects or resources on the network;
- e. **account monitoring** to log, monitor, and analyze account activity to ensure account permissions are used correctly and detect suspicious or unauthorized behavior;
- f. **privileged account management** to secure, monitor, and manage accounts with elevated access and activity permissions;
- g. **managed detection and response** to record, store, and analyze system level activity to detect, block, and report suspicious behavior;
- h. **governance, risk, and compliance** reviews to oversee policy, mitigate risk, and ensure legal compliance;
- i. **vendor assessments** to ensure its IT and security vendors were performing their services adequately, and

j. **responsibility assignment matrixes** to clearly establish the responsibilities of various participants in the information security business process.

25. Moreover, BCHP participated in a third party information security audit in 2023 that identified a number of security issues, including

- BCHP's lack of common information security policies and procedures,
- the lack of clarity regarding whether XTUM or BCHP was providing specific services to secure the BCHP information system,
- the lack of certain common standard security tools,
- the lack of an incident response plan, and
- the lack of a security vendor assessment program.

The 2023 information security audit provided BCHP with extensive findings and detailed suggestions for remediating the identified security concerns. BCHP did not reasonably respond to those audit findings, which contributed to the subsequent data breach.

26. In addition, multiple BCHP executives responsible for data security were aware for **over two years** before the 2024 breach that BCHP was hosting an unencrypted archive of over a million patient payment records containing protected information, including names, addresses, dates of birth, social security information, health insurance information, billing information, and treatment information. Despite this knowledge, the patient information archive remained essentially unprotected for years prior to being exfiltrated in the 2024 breach.

27. The unencrypted archive exfiltrated from BCHP contained the personal information of approximately 820,000 New Yorkers, including the social security number and driver's licenses of over 170,000 New York residents. Over 4,000 BCHP employee records containing protected information were also exfiltrated from a different database.

28. XTium and BChP cooperated in the investigation but at times provided incorrect, incomplete, or inconsistent information.

XTium and BChP's Conduct Violated New York Law

29. Executive Law § 63(12) prohibits illegal practices in the conduct of any business.

30. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. "Private information" includes, when unencrypted, an individual's name in combination with their driver's license number or social security number. GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

31. OAG finds that XTium and BChP's conduct violated Executive Law § 63(12) and GBL § 899-bb.

32. OAG finds that XTium and BChP's conduct violated the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C.

33. XTium and BChP neither admit nor deny OAG's Findings, paragraphs 1-32 above.

34. OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL § 899-bb based on the conduct described above.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

35. For the purposes of this Assurance, the following definitions shall apply:

- a. "API" means application programming interface.
- b. "Biometric Information" means data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity.
- c. "Consumer" shall mean any person residing in, or who has resided in New York.
- d. "Consumer Personal Information" shall mean Private Information and PHI of a Consumer.
- e. "Network" means any networking equipment, databases, data stores, applications, software, servers, endpoints, or other equipment or services that are capable of using, exchanging, or sharing software, data, hardware, or other resources and that are owned and/or operated by or on behalf of each Respondent.
- f. "Private Information" means private information as defined in New York General Business Law § 899-aa(1)(b).
- g. "Protected Health Information" or "PHI" shall mean health information, as defined in section 160.103 of title 45 of the Code of Federal Regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA").
- h. "Security Event" means unauthorized access to or acquisition of Consumer Personal Information collected, used, stored, retrieved, transmitted, displayed,

maintained, or otherwise processed by each Respondent.

GENERAL COMPLIANCE

36. Each Respondent shall comply with Executive Law § 63(12), and GBL § 899-bb, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D in connection with its collection, use, storage, retrieval, transmittal, display, maintenance, and other processing of Consumer Personal Information.

INFORMATION SECURITY PROGRAM

37. Each Respondent shall maintain and update a comprehensive information security program (“Information Security Program” or “Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Consumer Personal Information that each Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes. The Program shall be designed, modified, and implemented in accordance with the principles of zero trust architecture. Each Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include all the requirements detailed in paragraphs 40 to 50 and the following processes:

- a. Assess, update, and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Consumer Personal Information, including but not limited to all entries in the most recent Data Inventory (as defined by paragraph 41, *infra*);
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks each Respondent identified

that are appropriate to: (i) the size and complexity of each Respondent's operations; (ii) the nature and scope of each Respondent's activities; and (iii) the volume and sensitivity of the Consumer Personal Information that each Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes;

c. Assess, update, and document, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks to Consumer Personal Information each Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with this Assurance;

d. Test and monitor the effectiveness of such safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with this Assurance;

e. Assess, update as appropriate, and document, not less than annually, the Information Security Program and adjust the Program in light of any changes to each Respondent's operations or business arrangements, or any other circumstances that each Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

38. Each Respondent shall designate a qualified employee responsible for implementing, maintaining, assessing, updating, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The Chief Information Security Officer shall report at least quarterly to each Respondent's Chief Executive Officer (or the equivalent thereof)

and at least semi-annually to the Board of Directors (or the equivalent oversight entity if there is no Board of Directors) concerning each Respondent's Information Security Program. Such reports shall be in writing and include but not be limited to the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by each Respondent, and any barriers to the success of the Information Security Program.

39. Each Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, assessing, updating, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the Effective Date of this Assurance, or within thirty (30) days of when an employee first assumes new responsibility for implementing, maintaining, assessing, updating, or monitoring the Information Security Program. Each Respondent shall document that it has provided the notices and training required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

40. Account Access Management: Within ninety (90) days of the Effective Date of this Assurance, each Respondent shall, for all accounts, including but not limited to user accounts, service accounts, non-human accounts, or any other type of information system account, (i) utilize leading industry standard frameworks and templates to adopt or update

reasonable policies and procedures relating to the subjects below, and (ii) ensure such policies and procedures are appropriately enforced using leading industry standard tools and services:

- a. account permissions and restrictions;
- b. access segmentation;
- c. access control;
- d. account monitoring and logging;
- e. privileged account management;
- f. principle of least privilege;
- g. role based access control;
- h. access recertification;
- i. managed detection and response; and
- j. governance, risk, and compliance reviews.

41. Data Inventory: Within one-hundred and eighty (180) days of the Effective Date of this Assurance, each Respondent shall develop and maintain a data inventory of all instances in which it collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information. Each Respondent shall update and document its data inventory not less than annually. The data inventory shall, at a minimum, include the following processes:

- a. Identify all points at which Private Information is collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed;
- b. Map and/or track the complete path of all data flows involving Private Information, including API calls; and
- c. Ensure that reasonable safeguards are used to protect Private Information at all times.

42. Governance: Each Respondent shall maintain reasonable written policies, procedures, and documentation designed to ensure the security, integrity, and confidentiality of Consumer Personal Information. At least annually each Respondent shall:

a. Utilize leading industry standard frameworks and templates in adopting, reviewing, and updating such policies and procedures.

b. Document such review process, including the frameworks used, the templates reviewed, and the policies and procedures adopted, reviewed, updated, or rejected.

c. Maintain written documentation (i) clearly identifying each entity responsible for adopting, implementing, maintaining, monitoring, and updating all elements set out in the Information Security Program, and (ii) clearly identifying the roles and responsibilities of specific individuals responsible for executing each discrete element of the Information Security Program.

d. Provide detailed written notice to all such entities and individuals regarding their specific roles and responsibilities in ensuring the security, integrity, and confidentiality of Consumer Personal Information under such policies, procedures, and documentation.

43. Information Technology Service Vendors: Each Respondent shall maintain reasonable written policies and procedures designed to manage the risks associated with their use of, or performance as, information technology service vendors. At least annually, each Respondent shall utilize leading industry standard frameworks and templates in adopting, reviewing, and updating such policies and procedures, which shall include but not be limited to (as appropriate) vendor risk assessments and client risk assessments. Each Respondent shall

document such review process, including the frameworks used, the templates reviewed, and the policies and procedures adopted, reviewed, updated, or rejected.

44. Secure Software Development Lifecycle: To the extent each Respondent develops software, then they shall maintain reasonable written policies and procedures designed to ensure secure software development practices for and regular security assessments and testing of all web-based, mobile, or other applications—whether public-facing, credential-based, or internal—maintained by or on behalf of each Respondent that collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Consumer Personal Information. To the extent that a third-party is providing the application, each Respondent shall take reasonable steps to implement this requirement which may vary depending on the source of the application. Such policies and procedures must include the following requirements:

- a. Wherever Consumer Personal Information is implicated by the regular and expected use of any such application, each Respondent shall consider the privacy impact at each relevant stage of the software development lifecycle process;
- b. Wherever Consumer Personal Information is implicated by the regular and expected use of any such application, each Respondent shall include reasonably designed privacy testing and documented approval each time the application is changed or updated;
- c. For in-house software development personnel, provide periodic education on Consumer Personal Information, how such information can be used for fraud, and each Respondent's procedures, guidelines, and standards for protecting such information;

- d. For external software development vendors, evaluate, assess, and test adherence to each Respondent's secure development procedures, guidelines, and standards or reasonably equivalent secure development standards.

45. Authentication: Each Respondent shall maintain reasonable account management and authentication procedures, including the use of multifactor authentication (or a reasonably equivalent control), for access to Consumer Personal Information or remote access to each Respondent's Network. In addition, Respondent shall not allow any credentials to be accessed by more than one individual's account and all non-human accounts shall be inaccessible to human login.

46. Monitoring: Each Respondent shall maintain reasonable systems designed to collect and monitor Network activity, as well as activity on any platforms or applications operated by or on behalf of each Respondent, that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Consumer Personal Information. Each Respondent shall also establish and maintain reasonable policies and procedures designed to properly configure such tools to report anomalous activity. The systems shall, at a minimum: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for each Respondent's Network and any platforms or applications operated by or on behalf of each Respondent that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Consumer Personal Information, and (ii) monitor for and alert security personnel to suspicious activity. Activity logs should be immediately accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

47. Encryption: Respondents shall encrypt Consumer Personal Information that they collect, store, transmit, and/or maintain using an encryption method appropriate to the sensitivity of the Consumer Personal Information.

48. Segmentation: Respondents shall, to the extent they have not already done so, establish and implement, and thereafter maintain, policies and procedures designed to properly segment their networks and ensure that communication between partitions is permitted only to the extent necessary to meet business and/or operational needs.

49. Threat Response: Whenever each Respondent is aware of or reasonably should be aware of a reasonable risk of a Security Event, each Respondent shall:

- a. Promptly investigate and monitor for suspicious activity any platforms or applications operated by or on behalf of each Respondent and any places on its Network that collect, use, store, retrieve, transmit, display, or maintain, or otherwise process Consumer Personal Information; monitoring shall be at a level that is sufficiently granular to detect a potential Security Event;
- b. Promptly conduct a reasonable investigation to determine, at a minimum, whether Consumer Personal Information is exposed or otherwise at risk; and
- c. Promptly implement changes necessary to protect Consumer Personal Information at risk.

50. For the avoidance of doubt, to the extent that either Respondent contract with any third party to provide services subject to the provisions of this Assurance, such Respondent shall take reasonable steps to ensure that the material terms of this Assurance are satisfied.

INFORMATION SECURITY PROGRAM ASSESSMENTS

51. Within one hundred and eighty (180) days of the effective date of this Assurance, each Respondent shall obtain a comprehensive assessment of the information security of their networks conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Assessment Report") and provided to OAG within two weeks of completion.

52. Each respondent shall also, annually for three (3) years thereafter, obtain Third-Party Assessment Reports which Respondents shall maintain for six (6) years from the date of each Third-Party Assessment Report and shall provide to OAG upon request.

53. Each Respondent shall make available to the third-party assessor all information, documents, materials, and access that the third-party assessor reasonably requests in the performance of their assessment.

54. The third-party assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA), or a similarly qualified person or organization; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

55. The Third-Party Assessment Reports shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by Respondents' Information Security Program;

- b. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering Respondents' size and complexity, the nature and scope of Respondents' activities, the sensitivity of the Consumer Personal Information maintained on the networks and the reasonably anticipated risks;
- c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondents meet the requirements of the Information Security Program and the Assurance; and
- d. Make recommendations to enhance data security measures.

COMPLIANCE CERTIFICATION

56. BCHP shall provide OAG with a certification affirming its compliance with the requirements set forth in this Assurance, to be initially submitted to OAG within one year of the effective date of this Assurance. Thereafter, a certification of compliance shall be submitted to OAG on an annual basis for the following five (5) years and shall be provided within 90 days upon OAG's request for an additional four years. These certifications shall be in writing and signed under penalty of perjury by the Chief Executive Officer, the Chief Operating Officer, and the Chief Information Security Officer.

OAG ACCESS TO RECORDS

57. Each Respondent shall retain any documentation and reports required by paragraphs 37 to 56 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. For avoidance of doubt, this paragraph does not require each Respondent to provide the OAG with copies of any draft documents, draft reports, or communications that would otherwise be protected as attorney work product or under the attorney-client privilege.

MONETARY RELIEF

58. XTIUM and BCHP shall pay to the New York and Connecticut Attorneys General a total of four million dollars (\$4,000,000) in penalties and costs as follows:

- a. an initial payment of two million seven hundred thousand dollars \$2,700,000 by XTIUM and BCHP shall be paid in full within thirty (30) days of the effective date of this Assurance;
- b. the initial payment shall be divided and paid by Respondents directly to each of the Attorneys General in an amount designated by the Attorneys General;
- c. a second payment of one million three hundred thousand dollars (\$1,300,000) by BCHP shall be suspended; provided however, that the suspended amount will be immediately due and payable within 60 days if the OAG finds that BCHP materially breached this Assurance within 10 years of the date it is executed by the OAG;
- d. the second payment (if any) shall be divided and paid by BCHP directly to each of the Attorneys General in an amount designated by the Attorneys General;.

Payment shall be made in full within thirty (30) days of the effective date of this Assurance. Any payment to the OAG shall reference AOD No. 2026- 057.

MISCELLANEOUS

59. Each Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 66, and agrees and acknowledges that in such event:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;

- b. the OAG may use statements, documents or other materials produced or provided by each Respondent prior to or after the effective date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that each Respondent irrevocably and unconditionally waives any objection to such action or proceeding based upon personal jurisdiction, inconvenient forum, or venue;.
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

60. If a court of competent jurisdiction determines that a Respondent has violated the Assurance, such Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

61. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by any Respondent.

62. Acceptance of this Assurance by the OAG is not an approval or endorsement by OAG of any of a Respondent's policies, practices, or procedures, and a Respondent shall make no representation to the contrary.

63. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of a Respondent. Each Respondent shall include any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the

OAG.

64. Any failure by the OAG to insist upon the strict performance by a Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by a Respondent.

65. All notices, reports, requests, and other communications to OAG pursuant to this Assurance must reference Assurance No. 2026- 057, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to XTium, to:

Attn: Joshua H. Warmund, SVP, Legal Affairs & General Counsel, XTium, 4025 Tampa Road, Suite 1101, Oldsmar, FL 34677. Joshua.Warmund@xtium.com, or in their absence, to the person holding the same title

XTium.
4025 Tampa Road, Suite 1101
Oldsmar, FL 34677

If to BCHP, to:

Attn: Cari Ann Mondello, LMFT, Corporate Compliance Officer, Boston Children's Health Physicians, LLP, 400 Columbus Ave, Suite 200 East, Valhalla, NY 10595. CariAnn_Mondello@bchphysicians.org, or in their absence, to the person holding the same title

Boston Children's Health Physicians, LLP.
400 Columbus Ave, Suite 200 East
Valhalla, NY 10595

If to the OAG, to the person holding the title of Bureau Chief,

Attn: Bureau Chief
Bureau of Internet & Technology
The New York State Office of the Attorney General
28 Liberty Street, 16th Floor
New York, NY 10005

66. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by a Respondent and their counsel and the OAG's own factual investigation as set forth in Findings, paragraphs 1-32 above. Each Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by a Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

67. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by a Respondent in agreeing to this Assurance.

68. Each Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. XTUM further represents and warrants that XTUM, by Mike Pisterzi, President & CEO, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of XTUM. BHP further represents and warrants that Boston Children's Health Physicians, LLP, by Gerard M. Villucci, Chief Executive Officer, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of Boston Children's Health Physicians, LLP.

69. Nothing in this Agreement shall relieve a Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

70. Each Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects a Respondent's right to take legal or factual positions in defense of litigation or other legal proceedings to which the OAG is not a party.

71. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that a Respondent violates the Assurance after its effective date.

72. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

73. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

74. Each Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

75. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

76. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

77. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one

agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

78. The effective date of this Assurance shall be the date the OAG signs this Assurance.

BCHP

DocuSigned by:
By: Gerard M. Villucci
873750748127444...
Gerard M. Villucci, FACHE
Chief Executive Officer
Boston Children's Health Physicians, LLP
400 Columbus Avenue
Suite 200 East
Valhalla, NY 10595
Gerard_Villucci@bchphysicians.org

XTIUM

Signed by:
By: Mike Pisterzi
5452058E83F541D...
Mike Pisterzi
President & CEO
XTIUM
4025 Tampa Road
Suite 1101
Oldsmar, FL 34677
Mike.Pisterzi@xtium.com

Date: 10/15/2026 | 11:28 AM PDT

Date: 10/15/2026 | 8:06 PM EDT

LETITIA JAMES

Attorney General of the State of New York
28 Liberty Street
New York, NY 10005

By: _____
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology

Date: _____

agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

1. The effective date of this Assurance shall be the date the OAG signs this Assurance.

BCHP

XTIUM

By: _____
Gerard M. Villucci, FACHE
Chief Executive Officer
Boston Children's Health Physicians, LLP
400 Columbus Avenue
Suite 200 East
Valhalla, NY 10595
Gerard_Villucci@bchphysicians.org

By: _____
Mike Pisterzi
President & CEO
XTIUM
4025 Tampa Road
Suite 1101
Oldsmar, FL 34677
Mike.Pisterzi@xtium.com

Date: _____

Date: _____

LETITIA JAMES

Attorney General of the State of New York
28 Liberty Street
New York, NY 10005

By: Gena Feist
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology

Date: 10/16/26