

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

In the Matter of

Assurance No. 23-011

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

Heidell, Pittoni, Murphy & Bach LLP,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (the “OAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) §§ 899-aa and 899-bb as well as 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 (“HIPAA”) into a data security incident at Heidell, Pittoni, Murphy & Bach LLP (“HPMB” or “Respondent”) (together with the OAG, the “Parties”). This Assurance of Discontinuance (“Assurance”) contains the findings of the OAG’s investigation and the relief agreed to by the OAG and HPMB.

FINDINGS OF OAG

1. Respondent, HPMB, is a law firm based in New York, NY, that, among other things, represents hospitals and hospital networks in litigation. In connection with its role in representing hospitals and hospital networks in litigation, HPMB receives and maintains electronic protected health information (“ePHI”) and other private information related to its clients’ patients. As a result, HPMB was, at all relevant times, classified as a “Business Associate” under HIPAA and related regulations. *See* 45 C.F.R. §§ 160.103.

The 2021 Data Breach

2. On or about November 22, 2021, an attacker exploited vulnerabilities in HPMB's Hybrid Exchange Management Server to gain access to HPMB's systems. The vulnerabilities the attacker exploited had been identified by Microsoft several months earlier—in April and May 2021—and Microsoft had released patches for the software vulnerabilities around the same time. HPMB did not timely apply the patch for these vulnerabilities, rendering the server vulnerable to the attack.

3. On or around December 25, 2021, the attacker deployed the Lockbit ransomware variant on HPMB's systems using PSEXec. HPMB personnel were alerted to this intrusion on December 25, when HPMB received an internal alert relating to syncing errors. HPMB subsequently identified encryption on its network consistent with a ransomware attack.

4. In response to the attack, HPMB disconnected its servers from the internet and hired a forensic cybersecurity firm to conduct a forensic investigation. The forensic firm engaged in discussions with the attackers, who provided the forensic firm a list of tens of thousands of files the attackers claimed to have exfiltrated from HPMB's systems. This list included legal pleadings, patient lists, and medical records that HPMB had in its possession in connection with litigation matters. The forensic firm identified evidence that the listed files had been staged and exfiltrated from HPMB's systems.

5. HPMB subsequently paid \$100,000 in ransom in exchange for the return and promised deletion of the exfiltrated data but was not provided evidence the data was deleted.

6. With the aid of a contractor, HPMB engaged in an analysis of the files exfiltrated from its systems. As a result of this analysis, HPMB determined that the ePHI and/or private information—including names, dates of birth, social security numbers, and/or health data—of

114,979 individuals, including 61,438 New York residents, had likely been exposed as a result of the attack. Of this number, 846 New Yorkers had their social security numbers exposed, 23 New Yorkers had their driver's license numbers exposed, 13 New Yorkers had their other identification card details exposed, and 25 New Yorkers had their biometric data exposed.

7. On May 16, 2022, after HPMB's data-mining vendor had concluded its analysis of the exfiltrated files, Respondent began notifying affected individuals whose ePHI and private information had been exposed during the attack.

8. As a HIPAA Business Associate, HPMB must comply with the federal standards that govern the privacy and security of ePHI, as defined in 45 C.F.R. § 160.103—specifically, the HIPAA Privacy Rule and HIPAA Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E.

9. In the course of its investigation of the 2021 Data Breach, the OAG determined that HPMB failed to comply with many of the standards and procedural specifications required by HIPAA's Privacy Rule and Security Rule including, *inter alia*, the following:

- a. HPMB failed to ensure the confidentiality and integrity of all ePHI it creates, receives, maintains, or transmits, *see* 45 C.F.R. § 164.306(a)(1);
- b. HPMB failed to protect against reasonably anticipated threats or hazards to the security or integrity of such information, *see* 45 C.F.R. § 164.306(a)(2);
- c. HPMB failed to review and modify its data protection practices as needed to ensure reasonable and appropriate protection of ePHI, *see* 45 C.F.R. § 164.306(e);
- d. HPMB failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

- it holds, *see* 45 C.F.R. § 164.308(a)(1)(ii)(A);
- e. HPMB failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a), *see* 45 C.F.R. § 164.308(a)(1)(ii)(B);
 - f. HPMB failed to implement procedures to regularly review records of information system activity, *see* 45 C.F.R. § 164.308(a)(1)(ii)(D);
 - g. HPMB failed to implement procedures sufficient to guard against, detect, and report malicious software, *see* 45 C.F.R. § 164.308(a)(5)(ii)(B);
 - h. HPMB failed to implement procedures sufficient for periodic testing and revision of contingency plans, *see* 45 C.F.R. § 164.308(a)(7)(ii)(D);
 - i. HPMB failed to perform a periodic technical and nontechnical evaluation, based upon the standards implemented under the Security Rule and in response to environmental or operational changes affecting the security of ePHI, that established the extent to which its security policies and procedures meet the requirements of 45 C.F.R. Part 164, Subpart C, *see* 45 C.F.R. § 164.308(a)(8);
 - j. HPMB failed to sufficiently implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4), *see* 45 C.F.R. § 164.312(a)(1);
 - k. HPMB failed to implement a sufficient mechanism to encrypt and decrypt ePHI, *see* 45 C.F.R. § 164.312(a)(2)(iv);
 - l. HPMB failed to implement a centralized logging system that would allow it to record and examine activity in information systems that contain ePHI, *see* 45

C.F.R. § 164.312(b);

- m. HPMB failed to implement a system to identify whether PHI has been altered or destroyed in an unauthorized manner, *see* 45 C.F.R. § 164.312(c)(2);
- n. HPMB failed to implement procedures sufficient to verify that a person or entity seeking access to ePHI is the one claimed, *see* 45 C.F.R. § 164.312(d);
- o. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of 45 C.F.R. Part 164, Subpart C, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv), *see* 45 C.F.R. § 164.316(a);
- p. HPMB failed to prevent unauthorized access to the ePHI of individuals whose information was maintained on the HPMB Network, *see* 45 C.F.R. § 164.502(a); and,
- q. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the “minimum necessary” requirements for ePHI requests, use, and disclosure, *see* 45 C.F.R. § 164.502(b).

10. The OAG further finds that HPMB violated GBL § 899-aa by failing to provide affected New Yorkers with timely notice of the 2021 Data Breach and GBL § 899-bb(2) by failing to adopt reasonable data security practices to protect private information.

11. Respondent neither admits nor denies OAG’s Findings, paragraphs 1-10 above.

12. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of HIPAA, *see* 42 U.S.C. § 1320d-5(d), or Executive Law § 63(12) and GBL §§ 899-aa & 899-bb.

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

RELIEF

13. For the purposes of this Assurance, the following definitions shall apply:
- a. “Affected Consumer” means any person who resided in New York at the time of the Security Event and whose Private Information or ePHI was potentially subject to the Security Event.
 - b. “Effective Date” shall be the date of the last signature to this agreement.
 - c. “ePHI” or “Electronic Protected Health Information” has the same meaning as the same term in 45 C.F.R. § 160.103.
 - d. “Private Information” shall have the same meaning as the same term in New York General Business Law § 899-aa.
 - e. “Security Event” means the ransomware attack that occurred in December 2021 and resulted in unauthorized access to and acquisition of Private Information and ePHI maintained by HPMB.

GENERAL COMPLIANCE

14. Respondent shall comply with Executive Law § 63(12) and GBL §§ 899-aa & 899-bb as well as HIPAA’s Privacy Rule and Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E, in connection with its collection, use, and maintenance of ePHI and Private Information.

INFORMATION SECURITY PROGRAM

15. Respondent shall maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of the ePHI and Private Information that Respondent collects, stores, transmits,

and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

- a. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of ePHI and Private Information;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the ePHI and Private Information that Respondent collects, stores, transmits, and/or maintains;
- c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;
- d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;
- e. Select service providers capable of appropriately safeguarding ePHI and Private Information, contractually require service providers to implement and maintain appropriate safeguards to protect ePHI and Private Information, and take appropriate steps to verify service providers are complying with the contractual requirements;

- f. Evaluate the Information Security Program not less than annually and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

16. Respondent shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall report at a minimum quarterly to the Chief Executive Officer (or the equivalent thereof) and senior management concerning Respondent's security posture, the security risks faced by Respondent, and the Information Security Program. The Chief Information Security Officer shall report at a minimum semi-annually to the Board of Directors (or the equivalent thereof) regarding the same.

17. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, 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 responsibility for implementing, maintaining, or monitoring the Information Security Program.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

18. Encryption: Respondent shall encrypt ePHI and Private Information that it collects, uses, stores, transmits and/or maintains, whether stored within Respondent's network, or

transmitted electronically within or outside the Respondent's network, using a reasonable encryption algorithm where technically feasible.

19. Logging & Monitoring: Respondent shall, to the extent it has not already done so, establish, and, thereafter, maintain a system designed to programmatically collect and monitor network activity, such as through the use of security and event management tools, as well as policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondent's network, and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

20. Patch Management: Respondent shall implement and maintain a reasonable policy to update and patch software on its computer network including the following:

- a. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from software manufacturers and ensuring the appropriate and timely application of all security updates and/or security patches;
- b. Supervising, evaluating, and coordinating any system patch management tool(s); and,
- c. Training requirements for individuals responsible for implementing and maintaining Respondent's patch management policies.

21. Penetration Testing: Respondent shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within Respondent's computer network. This program shall include regular penetration testing,

risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

22. Data Collection: Respondent shall request, collect, use, or store ePHI and/or Private Information only to the minimum extent necessary to accomplish the intended legitimate business purpose for collection.

23. Data Deletion: Respondent shall permanently and securely delete or otherwise dispose of ePHI and/or Private Information when there is no reasonable business or legal purpose to retain it.

INFORMATION SECURITY PROGRAM ASSESSMENTS

24. Within one (1) year of the effective date, Respondent shall obtain a comprehensive assessment of the information security of the HPMB Network conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession (the “Third-Party Assessment”) which shall be documented (“Third-Party Assessment Report”) and provided to the OAG within two weeks of completion. Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Reports which shall be provided to the OAG upon request. The Third-Party Assessment Reports shall:

- a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent’s Information Security Program;
- b. Document the extent to which the identified administrative, technical and physical safeguards are appropriate based on the volume and sensitivity of the ePHI and Private Information that is at risk and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to ePHI or Private Information, or the (2)

misuse, loss, theft, alteration, destruction, or other compromise of such information; and,

- c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program.

CREDIT MONITORING

25. Respondent shall offer two (2) years of credit monitoring and identify theft protection services to all Affected Consumers who were impacted by the 2021 Data Breach and were not previously offered identify theft protection services.

MONETARY RELIEF

26. Respondent shall pay to the State of New York two hundred thousand dollars (\$200,000) in penalties (the “Monetary Relief Amount”). Payment of the Monetary Relief Amount shall be made in full within forty-five (45) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 23-011.

MISCELLANEOUS

27. 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 34, 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 the 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 Respondent irrevocably and unconditionally waives any objection 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).

28. If a court of competent jurisdiction determines that the Respondent has violated the Assurance, the 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.

29. This Assurance is not intended for use by any third party in any other proceeding.

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

31. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. 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.

32. Any failure by the OAG to insist upon the strict performance by 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 the Respondent.

33. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-011, 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 the Respondent, to:

Adam M. Dlugacz, or in his absence, to the person holding the title of
Managing Partner
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com

If to the OAG, to:

Laura Mumm, Assistant Attorney General, or in her absence,
to the person holding the title of Bureau Chief Bureau of
Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov

34. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and its counsel and the OAG's own factual investigation as set forth in Findings, paragraphs (1)-(10) above. The 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 Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

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

36. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that Heidell, Pittoni, Murphy & Bach, LLP, by Adam M. Dlugacz, as the signatory to this AOD, is a duly authorized officer and managing partner acting at the direction of the Executive Committee of Heidell, Pittoni, Murphy & Bach, LLP.

37. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

38. 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.

39. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its Effective Date.

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

41. 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.

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

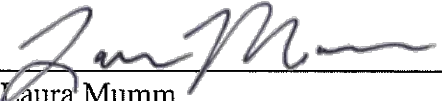
43. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

44. 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.

45. 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.

46. The Effective Date of this Assurance shall be March 10, 2023.

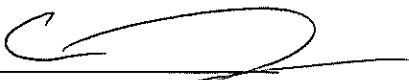
**LETITIA JAMES
ATTORNEY GENERAL OF THE STATE
OF NEW YORK**

By: 

Laura Mumm
Assistant Attorney General
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov
Phone: (212) 416-8276

Date: 3/9/2023

**HEIDELL, PITTONI, MURPHY &
BACH, LLP**

By: 

Adam M. Dlugacz
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com
Phone: (212) 286-8585

Title: Managing Partner

Date: 3/3/23