

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

In the Matter of

Assurance No. 23-010

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

Personal Touch Holding Corp.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“OAG”) commenced an investigation pursuant to New York Executive Law § 63(12), New York General Business Law (“GBL”) § 399-ddd, and New York GBL § 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 two data security incidents affecting Personal Touch Holding Corp. and its direct and indirect subsidiaries (collectively, “PTHC”). This Assurance of Discontinuance (“Assurance”) contains the findings of the OAG’s investigation and the relief agreed to by the OAG and PTHC (collectively, the “Parties”).

OAG’s FINDINGS

1. Respondent PTHC is a Delaware corporation with a principal place of business in Lake Success, NY. It is the parent company of direct and indirect subsidiaries that operate Medicare-certified home health, home care, and hospice at home services throughout the United

States and formerly the parent company of a managed long-term care provider (the “MLTC”) in New York that was sold in May 2022.

2. PTHC provides administrative services, such as human resources and other back office services, for all its subsidiaries. PTHC also provides information technology and data security for substantially all of its subsidiaries.

3. In connection with its role in providing administrative services for its subsidiaries, PTHC maintains electronic personal health information (“ePHI”) of its subsidiaries’ patients and personal information of its subsidiaries’ employees.

4. In 2016, PTHC entered into a private cloud and network management agreement with a managed service provider. Pursuant to this agreement, the managed service provider implemented and managed technical security requirements, among other things, according to PTHC’s direction. The managed service provider also provided advice and recommendations to PTHC.

The Ransomware Attack

5. On January 20, 2021, a PTHC employee opened a malicious Microsoft Excel file attached to a phishing email. Malicious software embedded in the Excel file was executed and gave the threat actor access to the PTHC employee’s laptop and account.

6. Using the PTHC employee’s account, the threat actor executed tools to escalate privileges and obtain domain administrator credentials that the threat actor then used to navigate the PTHC Network. A total of five accounts were compromised.

7. On January 27, 2021, the threat actor, using domain administrator credentials, collected files from a file share server containing PTHC employee and patient personal

information including ePHI, copied 4,383 unique files into ten RAR archives, and exfiltrated the data. The threat actor also viewed numerous additional folders on the file share server.

8. On January 27, 2021, after exfiltrating the data, the threat actor deployed ransomware, which encrypted 35 PTHC servers.

9. At the time of the intrusion, two anti-virus products were deployed within the PTHC Network: Microsoft Windows Defender (“Defender”) and Symantec Endpoint Protection (“Symantec”).

10. Both products detected and blocked many of the tools used by the threat actor, but Defender did not log to a central server, giving no visibility of these incidents beyond the local file system of the affected systems. Furthermore, while PTHC received Symantec reports for suspicious activity, the reports for the days leading up to the ransomware attack did not show any relevant suspicious activity.

11. PTHC became aware of the ransomware attack on the morning of January 27, 2021, when its managed service provider alerted PTHC that its systems were unavailable and discovered a ransomware note. PTHC shut down all systems the same day and, over the following several weeks, restored affected servers and replaced affected personal computers.

12. The PTHC file share server from which data was exfiltrated stored records from all lines of business and contained the personal information and ePHI of current and former patients and current and former employees of PTHC and its then-subidiaries. The affected file share server was used by office staff to store individual, work-related documents on an ad-hoc basis. The data stored on the file share server was not encrypted.

13. On March 24, 2021, PTHC provided notice of the breach to all current and former patients and all current and former employees of PTHC and its subsidiaries. In all, 753,107

individuals were notified, 316,845 of whom were New York residents.¹ The earliest patient record was from 1980, and the earliest employee record was from 1974.

14. PTHC sent a number of different notices to affected patients and employees, only some of whom received an offer of credit monitoring and identity theft recovery services:

a. *Patients*: Current and former patients of PTHC and its subsidiaries (except MLTC members) in New York were informed that their personal data may have been impacted, including first and last name, address, telephone numbers, date of birth, Social Security number, medical treatment information, insurance card and health plan benefit numbers, medical record numbers, and financial information, including check copies, credit card numbers, and bank account information. Current and former patients located in New York were not offered any credit monitoring or identity theft recovery services.

b. *Employees*: Current and former employees of PTHC and its subsidiaries (except the MLTC) in New York were informed that their personal data may have been impacted, including first and last name, address, telephone numbers, date of birth, Social Security numbers, driver's license number, background and credit reports, demographic information, personal email addresses, fingerprints, insurance card and health and welfare plan benefit numbers, retirement benefits information, medical treatment information, check copies, and other financial information necessary for payroll. Current and former employees in New York were offered one year of credit monitoring and identity theft recovery services through IDX.

c. *MLTC Members*: One set of current and former MLTC members in New York were informed that their impacted data may include first and last name and Medicaid ID number. They were not offered any credit monitoring or identity theft recovery services.

Another set of current and former MLTC members in New York were informed that their impacted data may include first and last name, address, telephone number, date of birth, Social Security numbers, Medicaid ID number, MLTC ID number, provider name, clinical/medical information, and credit card numbers and/or banking information. They were offered one year of credit monitoring and identity theft recovery services through IDX.

¹ Subsequent review indicated that the number of patients and employees whose data was exfiltrated was fewer than 52,000 nationwide. The number of patients and employees whose data was accessed remains unknown.

PTHC's Data Security Deficiencies

15. In the year leading up to the ransomware attack, PTHC had been made aware of several data security deficiencies and needed improvements.

16. Beginning in early 2020, PTHC's managed service provider recommended various security enhancements, including an Endpoint Detection and Response ("EDR") tool, which would improve upon existing anti-virus software by protecting against known and newly discovered threats; a Security Information and Event Management ("SIEM") solution, which would collect real-time log and event data generated from different devices and applications throughout the PTHC Network (defined below) into one centralized, network-wide platform; and improving IT governance beginning with a risk analysis and vulnerability scans and implementing a learning management system for user training.

17. In March 2020, an information security services company conducted a risk assessment of all of PTHC's computer systems, services, and applications.

18. The risk assessment identified the following five (5) high-risk control deficiencies:

- i. There was no continuous monitoring of the system and network security and no SIEM tool in place, which potentially allowed data breaches or other malicious activity to go undetected and left the organization vulnerable to privileged account abuse;
- ii. The Business Continuity and Disaster Recovery Plan and associated processes were inadequate; specifically, PTHC's electronic medical records ("EMR") system had limited redundancy controls in place, restoration from daily incremental backups had failed following a November 2019 security incident and PTHC had been forced to restore this critical application to a 14-day-old backup, and quarterly disaster recovery tests were performed on PTHC's EMR application and critical systems (phone, email, firewall, ISPs) but not the corporate network;

- iii. Control gaps existed with PTHC's managed service provider; for example, data retention policies were not adequately implemented and enforced, as email was archived indefinitely, presenting privacy risks to PTHC, and the security alerting process required maturity to ensure all pertinent, security-related information was relayed to PTHC;
- iv. IT Vendor Management practices were inadequate, as a formal program was not in place to ensure all critical third-party vendors were reviewed annually for compliance with PTHC's security requirements; and
- v. Multi-Factor Authentication ("MFA") was not utilized for (1) email access and (2) remote and EMR access.

19. The risk assessment also identified the following fourteen (14) moderate-risk control deficiencies:

- i. The vulnerability scanning process required further maturity, as PTHC did not routinely perform vulnerability scans against their production and testing environments;
- ii. Access controls were inadequate (in particular, user, group, and role permissions both at the user and system account level had not been reviewed in many years and password complexity requirements were at default values from the 2003 version of Active Directory), and users potentially did not have least privileged access;
- iii. Service account passwords did not expire, such that if a service account with privileged access were compromised, an attacker would be able to move through the environment undetected with domain-level access;
- iv. There was no learning management system to help administer and track security and privacy training;
- v. Email phishing tests were not conducted frequently enough;
- vi. PTHC had not completed a PCI self-assessment questionnaire, a requirement for PCI compliance;
- vii. There was no clearly defined privacy or security officer;
- viii. Wireless network controls were inadequate;

- ix. PTHC's formal risk management program and internal audit program required further maturity, as risk evaluations were informal and there was no centralized method of tracking risk and its remediation over time;
 - x. Employees could use personal devices to access company data (e.g., ePHI);
 - xi. Mobile device security settings were not enforced;
 - xii. Firewall rules were not routinely reviewed;
 - xiii. The incident response plan lacked sufficient detail and was not tested on a regular basis; and
 - xiv. PTHC did not have the ability to automatically detect unauthorized systems on its network.
20. PTHC's lack of MFA had been previously identified as high risk by a security company that conducted an external penetration test of PTHC's systems in September 2018.
21. PTHC had also conducted risk assessments in 2018 and 2019 by its own employees, which failed to identify the lack of MFA as a risk and failed to identify almost all of the other vulnerabilities identified in the March 2020 risk assessment.

The Employee Benefits Enrollment File

22. During the pendency of the OAG's investigation, PTHC notified the OAG of a third-party security incident affecting the personal information of PTHC employees.
23. On May 5, 2022, a former PTHC employee ran a Google search of themselves and discovered a publicly available spreadsheet containing the personal information of current and former PTHC employees, including Social Security Numbers.
24. This spreadsheet had been created in the fall of 2020, when PTHC provided employee data, including social security numbers, to its insurance broker, which in turn provided the data to vendors of PTHC's insurance provider.

25. An enrollment software vendor created a spreadsheet with this information (“Benefits Enrollment File” or the “File”) and, in December 2020, transferred it to PTHC by placing the File on its own File Transfer Protocol (“FTP”) site.

26. The security settings on the enrollment vendor’s site were misconfigured, which resulted in the Benefits Enrollment File being accessible to the public internet until the former PTHC employee discovered it in May 2022.

27. The former employee alerted PTHC, which in turn alerted the enrollment vendor.

28. The vendor immediately removed the File, then engaged a forensic firm to conduct an investigation. The forensic firm identified 20 instances of unauthorized access of the File during the period from October 13, 2021 to May 4, 2022.

29. The Benefits Enrollment File contained the full name, social security number, date of birth, and date of hire of 1,713 current and former PTHC employees and the full name, social security number, and home address of 833 dependents of those employees. A subset of the 1,713 impacted employees also had benefits eligibility and election, home phone number, personal email address, and job title included in the File.

30. PTHC did not have any agreements in place with its insurance broker concerning the data security standards the broker was required to meet when handling Private Information (defined below) not covered by HIPAA.

31. PTHC failed to document whether it had conducted any security diligence of its insurance broker.

32. PTHC did not have any agreements in place with its insurance provider concerning either (i) the data security standards the provider was required to meet when handling

Private Information or, (ii) the data security standards that the insurance provider must require subcontractors to meet when handling Private Information.

33. PTHC failed to conduct any formal security diligence of its insurance provider.

34. PTHC did not have any agreements in place with the enrollment vendor, relating to data security or otherwise.

Respondent's Violations

35. PTHC is, and at all relevant times was, a business associate to its direct and indirect subsidiaries, which are each individual covered entities pursuant to 45 C.F.R. § 103.

36. As a business associate, PTHC 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.

37. The OAG finds that, by its actions described above, PTHC violated GBL § 399-ddd(4) by failing to provide safeguards necessary or appropriate to preclude unauthorized access to Social Security account numbers and failing to protect the confidentiality of such numbers.

38. The OAG further finds that PTHC violated GBL § 899-bb(2) by failing to adopt reasonable data security practices to protect private information.

39. The OAG further finds that PTHC failed to comply with the following standards and procedural specifications required by HIPAA's Privacy Rule and Security Rule:

- i. PTHC 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);
- ii. PTHC 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);

- iii. PTHC 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);
- iv. PTHC 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);
- v. PTHC failed to implement procedures to regularly review records of information system activity, *see* 45 C.F.R. § 164.308(a)(1)(ii)(D);
- vi. PTHC failed to sufficiently implement policies and procedures that, based on its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process, *see* 45 C.F.R. § 164.308(a)(4)(ii)(C);
- vii. PTHC failed to implement procedures sufficient to guard against, detect, and report malicious software, *see* 45 C.F.R. § 164.308(a)(5)(ii)(B);
- viii. PTHC failed to implement procedures sufficient to restore data loss, *see* 45 C.F.R. § 164.308(a)(7)(ii)(B);
- ix. PTHC failed to implement procedures sufficient for periodic testing and revision of contingency plans, *see* 45 C.F.R. § 164.308(a)(7)(ii)(D);
- x. PTHC 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);

- xi. PTHC 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);
 - xii. PTHC failed to implement a mechanism to encrypt and decrypt ePHI, *see* 45 C.F.R. § 164.312(a)(2)(iv);
 - xiii. PTHC 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);
 - xiv. PTHC 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);
 - xv. PTHC failed to prevent unauthorized access to the ePHI of individuals whose information was maintained on the PTHC Network, *see* 45 C.F.R. § 164.502(a);
 - xvi. PTHC 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).
40. Respondent neither admits nor denies the OAG’s Findings, paragraphs 1-39 above.
41. 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 GBL

§ 399-ddd(4), GBL § 899-bb(2), and 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E.

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

PROSPECTIVE RELIEF

42. For the purposes of this Assurance, the following definitions apply:
- i. “Affected Consumer” means any person who resided in New York at the time of the Security Event and who was provided notice of the Security Event as described in ¶ 14.
 - ii. “CVSS” means the Common Vulnerability Scoring System established by the National Institute of Standards and Technology’s National Vulnerability Database.
 - iii. “ePHI” or “Electronic Protected Health Information” has the same meaning as the same term in 45 C.F.R. § 160.103.
 - iv. “MFA” or “Multifactor Authentication” means authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.
 - v. “Private Information” has the same meaning as the same term in New York General Business Law § 899-aa(1)(b).
 - vi. “PTHC Network” shall mean the networking equipment, databases or data stores, applications, servers, and endpoints that are capable of using and sharing

software, data, and hardware resources and that are owned and/or operated by or on behalf of PTHC.

- vii. “Security Event” means the ransomware attack that occurred in January 2021 and resulted in unauthorized access to and acquisition of Private Information and ePHI owned, licensed, or maintained by PTHC.

GENERAL COMPLIANCE

43. Respondent shall comply with GBL § 899-bb(2), 45 C.F.R. Part 160 and 45 C.F.R. Part 164, and 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 the security, collection, use, storage, transmission, and maintenance of ePHI and Private Information.

INFORMATION SECURITY PROGRAM

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

- i. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of ePHI and Private Information;
- ii. In order to control the internal and external risks identified by the risk assessment required by ¶ 44(i), design, implement, and maintain administrative, technical, and physical safeguards that are 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;

- iii. 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;
- iv. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results;
- v. 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.

45. Respondent shall designate a Chief Information Security Officer who must report at least quarterly to Respondent's Chief Executive Officer or, in the absence of a Chief Executive Officer, an appropriately designated Board Committee. The Chief Information Security Officer shall be responsible for implementing, maintaining, and monitoring the Information Security Program and have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, and monitoring the Information Security Program.

46. 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 within thirty (30) days of the effective date of this Assurance. For management-level employees responsible for implementing, maintaining, or monitoring the

Information Security Program after thirty (30) days from the effective date, Respondent shall provide notice of the requirements of this Assurance prior to, or immediately upon commencement of, the start of their duties.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

47. Asset Inventory: Respondent shall develop, maintain, and regularly update a reasonable inventory of PTHC Network assets that contain ePHI and Private Information.

48. Access Controls: Respondent shall implement and maintain appropriate access controls to manage access to ePHI and Private Information. Respondent shall regularly review and update user, group, and role permissions to ensure that users have the minimum access necessary to fulfill their roles and responsibilities. Respondent shall ensure that users with access to administrator accounts also maintain and use separate, standard user accounts for non-administrator work.

49. Authentication: Respondent shall maintain reasonable account management and authentication procedures, including the use of MFA (or a reasonably equivalent technology) for access to administrator accounts, remote access to the PTHC Network, and access to any systems in the PTHC Network containing ePHI or Private Information. For access to databases containing ePHI that are maintained by third-party vendors, Respondent shall enable MFA or a reasonably equivalent security measure to the extent made available by such third-party vendor. Respondent shall implement compensating controls to restrict access to cached account credentials.

50. Encryption: Respondent shall encrypt ePHI and Private Information that it collects, uses, stores, transmits and/or maintains, whether stored within the PTHC Network, or

transmitted electronically within or outside the PTHC Network, using a reasonable encryption algorithm.

51. Logging & Monitoring: Respondent shall establish and maintain a system designed to collect and monitor network activity, such as through the use of SIEM 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 the PTHC Network, and (2) monitor for and alert security personnel to suspicious activity. Respondent shall regularly test, update, and maintain such system. 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.

52. Anti-Malware Program: Respondent shall implement, maintain, and regularly monitor, test, and update reasonable anti-malware protections such as an EDR solution (or reasonably equivalent technology).

53. Intrusion Detection and Prevention Solution(s): Respondent shall implement, maintain, and regularly monitor, test, and update an intrusion detection and prevention solution to assist in detecting and preventing unauthorized access to the PTHC Network.

54. Email Filtering and Phishing Solutions: Respondent shall maintain and regularly monitor, test, and update email protection and filtering solutions for all email accounts connected to the PTHC Network, including tools to address email SPAM, phishing attacks, and malware. Respondent shall ensure that alerts from its email protection and filtering solutions log to a centralized platform.

55. Vulnerability Management: Respondent shall develop, implement, and maintain a vulnerability management program designed to identify, assess, and remediate security vulnerabilities within the PTHC Network. The program must include:

- i. Vulnerability scanning, or a reasonably equivalent technology;
- ii. Annual external and internal penetration tests or a reasonably equivalent technology, conducted by a qualified third party, the reports of which shall be maintained by the Chief Information Security Officer described in ¶ 45 responsible for the Information Security Program for at least five (5) years; and
- iii. Appropriate remediation of vulnerabilities revealed by such scanning and testing. Vulnerabilities with a CVSS rating of “Critical” (9.0-10.0) or that are listed on the Known Exploited Vulnerabilities Catalog (or any successor catalog) maintained by the U.S. Cybersecurity & Infrastructure Security Agency must be remediated within 30 days of Respondent’s discovery of the vulnerability or the vulnerability’s addition to the Known Exploited Vulnerabilities Catalog, whichever is sooner.

56. Data Minimization: Respondent shall collect, use, retain, and disclose ePHI and Private Information to the minimum extent necessary to accomplish Respondent’s legitimate business, medical, or legal purposes, unless otherwise permitted by HIPAA.

57. Data Retention and Disposal: Respondent shall establish, maintain, and regularly update policies and processes to ensure that any ePHI or Private Information is securely retained consistent with Respondent’s legitimate business, medical, or legal purposes and that the Private Information of Respondent’s employees and contractors is securely disposed of when the information is no longer needed for such purposes. Such policies and procedures shall include a retention schedule for the Private Information of Respondent’s employees and contractors that

specifies a set timeframe for deletion or disposal of each type of Private Information Respondent may collect and retain.

58. Data Deletion: Within ninety (90) days of the effective date of this Assurance, Respondent shall provide to the OAG a copy of the retention schedule required by ¶ 57 and certify that it has permanently and securely deleted or otherwise disposed of the Private Information of its employees and contractors in accordance with the retention schedule.

59. Employee Training: Respondent shall conduct an initial training for all new employees and, on at least an annual basis, train existing employees concerning its information privacy and security policies and the proper handling and protection of ePHI and Private Information. At a minimum:

- i. Respondent's new employee and annual training shall cover social engineering schemes, such as phishing;
- ii. Respondent shall conduct annual mock phishing exercises and all employees who fail must successfully complete additional training; and
- iii. Respondent shall document such trainings and the results of the mock phishing exercises.

60. Vendor Management: Respondent shall make reasonable efforts to ensure that any vendor that accesses, receives, stores, maintains, processes, or otherwise handles or uses ePHI or Private Information maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of such ePHI and Private Information. Such efforts must include, at minimum:

- i. Requiring such safeguards by contract with the vendor;
- ii. Requiring the vendor to require such safeguards by contract with any subcontractor

that accesses, receives, stores, maintains, processes, or otherwise handles or uses ePHI or Private Information on behalf of Respondent;

- iii. Conducting and documenting reasonable security diligence of the vendor prior to engagement and at least once every three years throughout the engagement.

INFORMATION SECURITY PROGRAM ASSESSMENTS

61. Within one (1) year of the effective date of this Assurance, Respondent shall obtain a comprehensive assessment of the information security of the PTHC 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:

- i. Identify the specific administrative, technical, and physical safeguards maintained by Respondent’s Information Security Program;
- ii. 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
- iii. 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 AND IDENTITY THEFT PROTECTION

62. Respondent shall offer, through direct notification, identity theft protection and recovery services to all Affected Consumers who were not previously offered such services. The offered identity theft protection and recovery services must cover a period of at least one (1) year and include, at a minimum, the following services:

- i. **Dark Web and Internet Scanning:** Daily proactive surveillance of the internet and dark web to seek out compromised personal information and providing alerts when such personal information is detected.
- ii. **Credit Monitoring:** Daily credit report monitoring from a nationwide consumer reporting agency (i.e., Equifax Information Services LLC, Experian Information Solutions, Inc., or TransUnion LLC) showing key changes to an Affected Consumer's credit report including automated alerts where the following occur: new accounts are opened; inquiries or requests for an Affected Consumer's credit report for the purpose of obtaining credit; changes to an Affected Consumer's address; and negative information, such as delinquencies or bankruptcies.
- iii. **Fraud Consultation and Identity Theft Restoration:** provide live support and explanation of the identity theft restoration process to ensure the victim understands his or her rights and responsibilities; investigate and resolve complicated trails of fraudulent activity; issue fraud alerts for the victim with the three consumer credit reporting agencies, the Social Security Administration, the Federal Trade Commission and the U.S. Postal Service; prepare appropriate documentation, from dispute letters to defensible complaints; work all identity theft issues until they have been verifiably resolved with all the organizations impacted including financial

institutions, collections agencies, check clearinghouse companies, landlords, property managers, and government entities; and

- iv. For Affected Consumers who are minors as of the notification date, an identity theft protection and recovery service appropriate for minors that includes the services listed in ¶¶ 62(i)-(iii), except that in lieu of Credit Monitoring, the service shall include credit file detection. For these Affected Consumers, direct notification shall be made to the Affected Consumer's parent or guardian.

MONETARY RELIEF

63. Respondent shall pay to the State of New York \$350,000 in penalties (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in full within 15 business days of the effective date of this Assurance. Any payment shall reference AOD No. 23-010.

MISCELLANEOUS

64. 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 71, 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).

65. 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.

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

67. 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.

68. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

69. 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.

70. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-010, 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:

Ronald Spielberg, or in the event of his absence, to the person holding the title of General Counsel.

Personal Touch Holding Corp.
1985 Marcus Avenue, Suite 202
Lake Success, NY 11042

If to the OAG, to:

Hanna Baek, or in the event of her absence, to the person holding the title of Bureau Chief, Bureau of Internet and Technology.

28 Liberty Street
New York, NY 10005

71. 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 their counsel and the OAG's own factual investigation as set forth in its Findings, paragraphs 1-39 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.

72. 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.

73. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

74. The obligations set forth in Paragraphs 48-55 of this Assurance shall expire at the conclusion of the seven (7) year period after the effective date. Provided, however, that nothing in this Paragraph shall be construed as excusing or exempting Respondent from complying with any state or federal law, rule, or regulation.

75. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Provided, however, that the content of the employee training required by paragraph 59 may be changed and updated in keeping with relevant cybersecurity regulations, threats, and guidance.

76. 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 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.

77. 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.

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

79. 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.


80. Respondent acknowledges that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

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

82. 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.

83. 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.

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

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By: _____ Hanna Baek Jina John Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 Fax: (212) 416-8369 <u>10/13/2023</u> Date</p>	<p>PERSONAL TOUCH HOLDING CORP.</p> <p>By:  Ronald J. Spielberger General Counsel & Chief Compliance Officer Personal Touch Holding Corp. 1985 Marcus Avenue, Suite 202 Lake Success, NY 11042 Phone: 718-468-4747</p> <p>_____ Date 10/2/23</p>
--	--