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

In the Matter of

Assurance No. 23-019

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

Professional Business Systems, Inc.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to New York General Business Law ("GBL") §§ 899-aa, 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 the data privacy and security practices of Professional Business Systems, Inc., d/b/a Practicefirst Medical Management Solutions and PBS Medcode Corp. (collectively, "Practicefirst"). This Assurance of Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and Practicefirst (collectively, the "Parties").

OAG FINDINGS

1. Respondent Practicefirst is a corporation with a principal place of business in Amherst, NY. Practicefirst is a medical management company hired by medical providers for medical billing, revenue cycle management, professional licensure credentialing, and medical practice management solutions.

2. In connection with its role in providing administrative services for its clients, Practicefirst maintains the protected health information ("PHI") and private information of individuals who are patients of its clients.

3. On January 31, 2019, Practicefirst's firewall provider released a new version of its software patching a critical firewall vulnerability. This vulnerability, unbeknownst to Practicefirst, was present in Practicefirst's systems.

4. Between May 2019 and August 2019, the firewall provider published an advisory for the vulnerability, the National Institute of Standards and Technology's National Vulnerability Database ("NVD") published an entry about the vulnerability, security researchers presented about the vulnerability at a Black Hat security conference, and a Metasploit module demonstrating the exploitation of the vulnerability was published online.

5. Between May 2019 and December 2020, Practicefirst and its managed service provider did not conduct any penetration tests, vulnerability scans, or other security testing that would have identified the vulnerability.

6. On or around November 25, 2020, an unauthorized actor exploited the critical firewall vulnerability to gain access to Practicefirst's systems.

7. From November 25, 2020 onwards, the unauthorized actor made several remote connections. The unauthorized actor used legitimate administrator accounts and further created an unauthorized domain administrator account to conduct malicious activity.

8. After several attempts, on December 24, 2020, the unauthorized actor successfully ran an open-source utility that enabled the unauthorized actor to view and harvest account credentials.

9. On December 25, 2020, Practicefirst's managed service provider identified suspicious activity on Practicefirst's system, including file extensions that had been changed and a ransom note.

10. Practicefirst subsequently shut down its systems and retained a cybersecurity firm to conduct a forensic investigation.

11. On December 30, 2020, Practicefirst confirmed that an unauthorized actor had deployed ransomware and had exfiltrated files containing personal information. The cybersecurity firm identified four screenshots containing the PHI and private information of thirteen individuals on the dark web.

12. On December 31, 2020, Practicefirst began communicating with the unauthorized actor, who then removed the four screenshots from the dark web that day.

13. From December 31, 2020 – January 4, 2021, Practicefirst notified 114 clients with which it had business associate agreements pursuant to HIPAA about the breach.

14. On January 9, 2021, Practicefirst paid the ransom and obtained a written attestation that the unauthorized actor had destroyed the exfiltrated data. The unauthorized actor provided information indicating 80 gigabytes of data, containing 79,000 files, were exfiltrated.

15. On January 28, 2021, the cybersecurity firm began reviewing the exfiltrated files.

16. On February 26, 2021, Practicefirst, at the direction of its clients, notified thirteen affected individuals about the breach. These individuals were identified through the screenshots the unauthorized actor posted on the dark web.

17. On February 27, 2021, Practicefirst notified the OAG about the breach and that thirteen affected individuals had been identified at that time.

18. On May 5, 2021, the cybersecurity firm completed its investigation and determined the unauthorized actor exfiltrated files containing the PHI and/or private information of over 1.2 million individuals, including over 428,000 New York residents. Furthermore, the data maintained on Practicefirst's network was not encrypted.

19. From May 6, 2021, Practicefirst coordinated with its clients regarding consumer notification.

20. From June 30 through July 2, 2021 Practicefirst, at the direction of its clients, notified the remaining 1.2 million affected individuals. Practicefirst provided direct notice to approximately 500,000 individuals and relied on substitute notice for the remaining affected individuals.

21. On July 1, 2021, Practicefirst submitted a second breach notice to the OAG providing an update on the scope of the breach.

22. In its consumer notices, Practicefirst informed affected individuals that their impacted data may include address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, tax identification number, employee username with password, employee username with security questions and answers, and bank account and/or credit card/debit card information. Practicefirst offered identity monitoring services to the affected individuals who received direct notice.

23. The OAG's investigation identified several areas where Practicefirst failed to maintain reasonable data security practices to protect consumer's private information, including:

i. Security Updates/Patch Management: Practicefirst failed to ensure system security updates were implemented on critical infrastructure. The recommended

security updates for the critical vulnerability that was exploited were made public in 2019. However, Practicefirst failed to patch the vulnerability until February 25, 2021, two months after the data breach and nearly two years after software updates were available.

ii. Account Authentication: Practicefirst failed to maintain appropriate account authentication measures, such as multi-factor authentication ("MFA"), that could have prevented the unauthorized actor from using administrator accounts to navigate through the Practicefirst network.

iii. Logging and Monitoring: Practicefirst failed to maintain appropriate logging and monitoring practices. In particular, Practicefirst failed to identify and address security alerts related to attempts to access and exfiltrate data from Practicefirst's network.

iv. Vulnerability Management: Practicefirst failed to conduct adequate security testing, including penetration tests and vulnerability scans that may have identified the firewall vulnerability prior to the data breach.

v. Encryption: Practicefirst failed to encrypt the files maintained on its network, potentially exposing the personal information, including protected health information and private information, of over 1.2 million individuals.

vi. Anti-Malware: Practicefirst failed to maintain an appropriate anti-malware program, including endpoint detection tools that may have prevented the unauthorized actor from running a malicious tool to extract account credentials.

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

25. Practicefirst is, and at all relevant times was, a business associate to its clients, which are each a covered entity pursuant to 45 C.F.R. § 103.

26. As a business associate, Practicefirst must comply with the federal standards that govern the security of PHI, as defined in 45 C.F.R. § 160.103—specifically, the HIPAA Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

27. The OAG finds that Practicefirst failed to comply with the following standards and procedural specifications required by HIPAA's Security Rule:

i. Practicefirst failed to ensure the confidentiality and integrity of all PHI it creates, receives, maintains, or transmits, *see* 45 C.F.R. § 164.306(a)(1);

ii. Practicefirst 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. Practicefirst failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI it holds, *see* 45 C.F.R. § 164.308(a)(1)(ii)(A);

iv. Practicefirst 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. Practicefirst failed to implement procedures to regularly review records of information system activity, *see* 45 C.F.R. § 164.308(a)(1)(ii)(D);

vi. Practicefirst failed to implement procedures sufficient to guard against, detect, and report malicious software, *see* 45 C.F.R. § 164.308(a)(5)(ii)(B);

vii. Practicefirst failed to implement procedures sufficient for periodic testing and revision of contingency plans, *see* 45 C.F.R. § 164.308(a)(7)(ii)(D);

viii. Practicefirst 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 PHI, 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);

ix. Practicefirst failed to sufficiently implement technical policies and procedures for electronic information systems that maintain PHI 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);

x. Practicefirst failed to implement a mechanism to encrypt and decrypt PHI, *see* 45 C.F.R. § 164.312(a)(2)(iv);

xi. Practicefirst failed to implement procedures sufficient to verify that a person or entity seeking access to PHI is the one claimed, *see* 45 C.F.R. § 164.312(d);

xii. Practicefirst 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);

xiii. Practicefirst failed to prevent unauthorized access to the PHI of individuals whose information was maintained on the Practicefirst Network, *see* 45 C.F.R. § 164.502(a);

28. The OAG further finds that Practicefirst violated GBL § 899-aa(2) by failing to notify affected individuals "in the most expedient time possible and without unreasonable delay"

after discovery of the breach. Most affected individuals were notified over six months after the breach.

29. Respondent neither admits nor denies the OAG's Findings, paragraphs 1-28 above.

30. 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 §§ 899-aa, 899-bb, 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

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

i. "Affected Individual" means any person who resided in New York at the time of the Security Event and whose PHI or Private Information was potentially subject to the Security Event.

ii. "Effective Date" shall be the date of the last signature to this Assurance.

iii. "Practicefirst 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 Practicefirst.

iv. "Private Information" has the same meaning as the same term in New York General Business Law § 899-aa(1)(b).

v. "Protected Health Information" or "PHI" has the same meaning as the same term in 45 C.F.R. § 160.103.

vi. "Security Event" means the ransomware attack that occurred in December 2020 and resulted in unauthorized access to and acquisition of Private Information and PHI owned, licensed, or maintained by Practicefirst.

GENERAL COMPLIANCE

32. Respondent shall comply with GBL §§ 899-aa, 899-bb and HIPAA's Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C, in connection with the security, collection, use, storage, transmission, and maintenance of PHI and Private Information.

INFORMATION SECURITY PROGRAM

33. Respondent shall maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PHI 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 PHI and Private Information;

ii. In order to control the internal and external risks identified by the risk assessment required by ¶ 33 (i), design, implement, and maintain administrative, technical, and physical safeguards that are based on the volume and sensitivity of the PHI 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 PHI 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.

34. Respondent shall designate a Chief Information Security Officer who must report to Practicefirst's CEO quarterly. The Officer will 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.

35. 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 and/or at least thirty (30) days prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

36. Encryption: Respondent shall encrypt PHI and Private Information that it collects, uses, stores, transmits and/or maintains, whether stored within the Practicefirst Network, or transmitted electronically within or outside the Practicefirst Network, using a reasonable

encryption algorithm where technically feasible or otherwise implementing compensating controls to protect such information from unauthorized access.

37. 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 Practicefirst Network, and access to any systems containing PHI or Private Information.

38. 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: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for the Practicefirst Network, and (ii) 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.

39. Intrusion Detection and Prevention: Respondent shall implement, maintain, and regularly monitor, test, and update a reasonable intrusion detection and prevention system including, but not limited to, an endpoint detection and response ("EDR") solution (or reasonably equivalent technology), host-based firewalls, network intrusion prevention systems, and a demilitarized zone.

40. Patch Management: Respondent shall adopt and maintain a reasonable patch management solution to manage software patches that includes the use of automated, standardized patch management distribution tool(s) to maintain a database of patches, deploy patches to endpoints, verify patch installation, and retain patch history. Respondent shall employ

processes and procedures to ensure the timely scheduling and installation of any security update and security patch, considering the severity of the vulnerability for which the update or patch has been released to address.

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

i. Monthly vulnerability scanning, or a reasonably equivalent technology;

ii. Annual external and internal penetration tests or a reasonably equivalent technology, conducted by an independent third party, the reports of which shall be maintained by the Chief Information Security Officer for at least five (5) years; and

iii. Appropriate remediation of vulnerabilities revealed by such scanning and testing. Vulnerabilities with a NVD Common Vulnerability Scoring System 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, or otherwise mitigated, promptly, and in no event later than 48 hours after Respondent's discovery of the vulnerability or 15 days after the vulnerability's addition to the Known Exploited Vulnerabilities Catalog.

42. Data Collection: Practicefirst shall request, collect, use, or store personal information, including PHI and Private Information, only to the minimum extent necessary to accomplish the intended legitimate business purpose for collection, or as otherwise permitted under 45 CFR § 164.502(b)(2).

43. Data Disposal: Practicefirst shall securely dispose of personal information, including PHI and Private Information, when there is no longer a business purpose or legal requirement for retention.

INFORMATION SECURITY PROGRAM ASSESSMENTS

44. Within one (1) year of the Effective Date, Respondent shall obtain a comprehensive assessment of the information security of the Practicefirst 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 fourteen (14) days of completion. Annually for four (4) years thereafter, Respondent shall obtain a Third-Party Assessment conducted by a qualified third-party assessor who uses procedures and standards generally accepted in the profession, which shall be documented in a Third-Party Assessment Report and 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 PHI 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 PHI 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 AND IDENTITY THEFT PROTECTION

45. Respondent shall offer identity theft protection and recovery services to all Affected Individuals. Notice of the offer for identity theft protection and recovery services shall be posted clearly and conspicuously on Practicefirst's website for a period of ninety (90) days from the Effective Date. The offered identity theft protection and recovery services must cover a period of at least two (2) years 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 Individual's credit report including automated alerts where the following occur: new accounts are opened; inquiries or requests for an Affected Individual's credit report for the purpose of obtaining credit; changes to an Affected Individual'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 their 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. Social Security Number trace for minors.

MONETARY RELIEF

46. Respondent shall pay to the State of New York $550,000 in penalties (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in full within 10 business days of the Effective Date of this Assurance. Any payment shall reference Assurance No. 23-019.

MISCELLANEOUS

47. 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 54, 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; and

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).

48. 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.

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

50. 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.

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

52. 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.

53. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-019, 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:

Thomas A. Maher
President & CEO
(or in his absence, to the person holding the title of CEO)
Practicefirst Medical Management Solutions
275 Northpointe Parkway, Suite 50
Amherst, NY 14228

With a copy to:

Brian H. Myers
Octillo Law PLLC
420 Main Street, Suite 1110
Buffalo, NY 14202
bmyers@octillolaw.com

If to the OAG, to:

Jina E. John
Assistant Attorney General
(or in her absence, to the person holding the title of Bureau Chief)
Bureau of Internet & Technology
New York State Office of the Attorney General
28 Liberty Street
New York, NY 10005

54. 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 the Findings, paragraphs 1-28 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.

55. 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.

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

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

58. 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.

59. 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.

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

61. 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.

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

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

64. 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.

65. 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.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

LETITIA JAMES **ATTORNEY GENERAL OF THE STATE OF NEW YORK** By: _____ Jina E. John Assistant Attorney General Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 _____ Date	**PROFESSIONAL BUSINESS SYSTEMS, INC., d/b/a PRACTICEFIRST MEDICAL MANAGEMENT SOLUTIONS AND PBS MEDCODE CORP.** By: _____ Thomas A. Maher President & CEO 275 Northpointe Parkway, Suite 50 Amherst, NY 14228 4/19/23 Date