STATE OF CONNECTICUT
OFFICE OF THE ATTORNEY GENERAL

ASSURANCE OF VOLUNTARY COMPLIANCE

The Attorney General of the State of Connecticut ("Attorney General") conducted an investigation under state consumer protection and privacy laws into a data security incident involving Perry Johnson & Associates, Inc. ("PJ&A"), Perry Johnson, Inc. ("PJI"), Perry Johnson & Associates Coding, Inc. ("PJ&A Coding"), Perry Johnson & Associates Radiology, Inc. ("PJ&A Radiology"), and Medical Transcription and Coding, Inc. ("MTC") (collectively, the "Respondents") that resulted in the exfiltration of sensitive data, including Social Security numbers and medical information, of approximately 13.3 million consumers nationwide, including approximately 107,960 Connecticut residents. This Assurance of Voluntary Compliance ("Assurance") contains the findings of the investigation and the relief agreed to by the Attorney General and Respondents, whether acting through their respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").[1]

I. INTRODUCTION

1. The Attorney General is the chief legal officer for the State of Connecticut. The Attorney General, in conjunction with the Connecticut Commissioner of Consumer Protection, is authorized to enforce violations of the Connecticut Unfair Trade Practices Act ("CUTPA"), as set forth in Conn. Gen. Stat. § 42-110a, *et seq*. Further, the Attorney General is authorized to enforce

[1] The investigation was conducted with the Offices of the Attorneys General of Connecticut, Michigan, and New Jersey (collectively, the "Attorneys General"). Respondents are entering into an Assurance with each of the Attorneys General, and each Attorneys General's Assurance incorporates the substantive terms included herein. To the extent there are differences, those arise from local rules, state laws, and Office requirements. The Connecticut Attorney General is acting on his own behalf and as authorized by the Commissioner of the Department of Consumer Protection.

the Connecticut Data Breach Notification Law ("Data Breach Notification Law"), Conn. Gen. Stat. 36a-701b, and Connecticut Safeguards Law, Conn. Gen. Stat. § 42-471 ("Safeguards Law"). The Attorney General is also authorized to enforce the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 101 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 ("HIPAA").

2. Perry Johnson Respondents PJ&A, PJ&A Coding, PJ&A Radiology, provided health information technology services to health care organizations across the country, including in Connecticut. PJ&A provided a variety of services, including medical transcription, coding, billing, recording, digital dictation, and court reporting services. PJ&A Coding and PJ&A Radiology provided diagnostic coding for insurance and telehealth radiology, respectively. Respondent MTC licensed health care software to Respondent PJ&A. Respondent PJI provided administrative and technical support services to PJ&A, PJ&A Coding, PJ&A Radiology, and MTC.

3. Respondents provided these services until approximately August 2024.

II. FINDINGS

The PJ&A and PJI Data Breach

4. In March 2023, PJ&A and PJI systems were targeted in a cyberattack. Threat actors gained initial access to the PJ&A network by remotely logging in through the RD Web application using credentials for a PJ&A Coding employee account. At the time, PJ&A did not require users to provide multi-factor authentication when remotely accessing PJ&A systems.

5. Over the next month, the threat actors engaged in network reconnaissance, password harvesting, privilege escalation, and lateral movement. The threat actors also accessed a variety of PJI and PJ&A systems and files that contained personal information and protected health information ("PHI"), including backup database files and files stored in shared network space. These files were not encrypted at the file level.

6. At the time of the attack, PJI maintained software to monitor for malicious activity on PJI and PJ&A systems. This software identified and recorded the threat actors' malicious activity at least as early as March 29, 2023. However, PJI and PJ&A had improperly configured the software to provide alerts to security personnel and so were not aware of the attack.

7. PJI and PJ&A personnel knew or should have known that the software had not been configured to provide alerts. In February 2022, a PJ&A system administrator contacted a PJI system administrator and asked whether the monitoring software, which PJI managed, was capable of sending out email alerts. After the PJI employee acknowledged the software had that capability, the PJ&A employee specifically requested that PJI configure the monitoring software to send out alerts by email. This was not done.

8. PJI and PJ&A did not become aware of the attack until May 2, 2023, when employees of the companies were contacted by the threat actors. The threat actors stated they had obtained tens of thousands of files from the network and demanded payment for their deletion.

9. On May 2, 2023, counsel for PJI engaged a cybersecurity firm to support the company's investigation of the incident. The investigation found that threat actors initially accessed the network through the RD Web application using compromised credentials, and confirmed that the threat actors had exfiltrated database files that contained patient information.

The investigation was not able to determine how threat actors obtained the compromised credentials.

10. In July 2023 PJ&A began contacting clients concerning the exfiltrated database files. Subsequent analysis showed that the database files contained records associated with more than 13.3 million individuals, approximately 107,960 of which were Connecticut residents. The database files contained a variety of personal information and PHI, including names, dates of birth, home addresses, medical record numbers, hospital account numbers, admission diagnoses, date(s) and time(s) of service, Social Security Numbers, insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, the names of medications, the names of the treatment facilities, and the names of healthcare providers.

11. Although the threat actors also accessed files stored on PJ&A and PJI shared network space that contained personal information and PHI, PJ&A and PJI did not review these files to identify additional individuals who were impacted in the incident.

12. PJ&A clients provided notice to individuals who had been impacted in the breach between October 31, 2023 and February 8, 2024.

PJ&A and PJI Password Management

13. As noted above, PJ&A and PJI could not determine how threat actors obtained credentials to the account used to initially access PJ&A systems. However, PJ&A and PJI accounts were vulnerable to compromise because the companies had failed to implement appropriate password management policies and procedures. Indeed, the companies had failed to comply with their own password management policies in several respects.

14. The PJ&A Coding user account that threat actors initially used to access PJ&A systems was one of nine accounts created by a PJ&A system administrator on May 6, 2022. At the time the accounts were created, the PJ&A system administrator assigned each account a password. The passwords for all nine accounts were nearly identical, with only the last character – a digit – differing.

15. After creating the accounts, the PJ&A system administrator then distributed the credentials for the nine accounts via email. Instead of sending the credentials for each account separately to each of the nine accountholders, however, the system administrator listed the credentials for all nine accounts in a single email that was sent to several managers. These managers then forwarded the email to the accountholders.

16. This method of distributing passwords is inherently insecure. It was also inconsistent with PJ&A password policies, which stated that "Administrators must not communicate passwords via email or other electronic communication."

17. In addition, when the email that contained the passwords was sent, the PJ&A system administrator inadvertently included the email address of an employee at another company. While the system administrator quickly realized his error, he did not revoke the account credentials. Instead, he merely forwarded the email to the originally intended recipient.

18. Moreover, although account credentials were forwarded by email, PJ&A did not require, or even permit, accountholders to change their credentials when first logging in. Nor did PJ&A automatically require accountholders to change their credentials at regular intervals. Indeed, even when the security breach occurred in March 2023 – 10 months later – the passwords

to the nine accounts remained the same. This was contrary to PJ&A policy, which required that passwords change every 90 days.

19. PJI's password management policies similarly required the regular rotation of user account passwords. However, password rotation was disabled for the two PJI accounts compromised in the attack.

Respondents' Data Security Programs

20. At the time of the attack in March 2023, Respondents' data security programs were deficient in several areas. These included:

a. Access Controls and Authentication: PJ&A and PJI failed to implement and maintain appropriate controls to limit access to sensitive data, including failing to use multi-factor authentication for all remote access, assigning account credentials in an insecure manner, distributing account credentials in an insecure manner, failing to rotate account credentials, and failing to restrict employees' access to only those resources and data necessary for their business functions.

b. Protection of Sensitive Information: PJ&A failed to encrypt, at the file level or below, all sensitive patient data maintained at rest.

c. Audit Controls and Monitoring: PJ&A and PJI failed to implement appropriate controls for monitoring user activity on its network.

d. Information Security Policies: PJ&A and PJI failed to adhere to written policies governing information security.

e. Risk Management and Testing: PJI failed to conduct a reasonable investigation to identify personal information and PHI maintained on its network.

Respondents' Compliance with the HIPAA Security Rule

21. The HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, sets forth requirements that covered entities and business associates must follow to secure electronic protected health information (ePHI). These include administrative, physical, and technical safeguards that must be put in place. PJ&A, PJ&A Coding, and PJ&A Radiology were "business associates" subject to the HIPAA Security Rule and these requirements.

22. To help ensure that covered entities and business associates maintain appropriate safeguards, the HIPAA Security Rule requires that these entities "perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements" of the HIPAA Security Rule. 45 CFR § 164.308(a)(8). These evaluations are typically conducted as part of the HIPAA risk analysis and risk management process. 45 CFR § 164.308(a)(1)(ii).

23. PJ&A, PJ&A Coding, and PJ&A Radiology conducted general risk assessments but never conducted a HIPAA risk analysis or evaluated the companies' administrative, technical, or physical safeguards in the context of the HIPAA Security Rule requirements, in violation of the HIPAA Security Rule.

24. PJ&A, PJ&A Coding, and PJ&A Radiology also failed to comply with HIPAA Security Rule requirements concerning the use of subcontractors. HIPAA only permits a business associate to disclose ePHI to a subcontractor if the subcontractor has agreed in writing to appropriately safeguard that ePHI. 45 CFR §§ 164.308(b), 164.314(a).

25. Despite this requirement, PJ&A, PJ&A Coding, and PJ&A Radiology allowed PJI to have technical access to systems containing PHI without contractually requiring PJI to maintain the confidentiality of, or use reasonable safeguards to protect, ePHI.

26. PJ&A, PJ&A Coding, and PJ&A Radiology, violated the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the HIPAA Breach Notification Rule, 45 C.F.R. Part 164 Subpart D, including:

a. § 164.308(a)(1)(i), which requires policies and procedures to prevent, detect, contain, and correct security violations;

b. § 164.308(a)(1)(ii)(A) and (B), which require an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI, and implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a);

c. § 164.308(a)(1)(ii)(D), which requires procedures to regularly review records of information system activity;

d. § 164.308(a)(4)(i), which requires policies and procedures for authorizing access to ePHI;

e. § 164.308(a)(4)(ii)(B) and (C), which require policies and procedures for granting access to ePHI, and establishing, documenting, reviewing, and modifying user's right of access based on access authorization policies;

f. § 164.308(a)(5)(ii)(C) and (D), which require procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords;

g. § 164.308(a)(6), which requires identifying and responding to security incidents and mitigating, to the extent practicable, harmful effects of security incidents;

h. §164.308(a)(7)(ii)(D), which requires implementation of procedures for periodic testing and revision of contingency plans, or documentation as to why the implementation of such procedures were not reasonable or appropriate, and implementation of an equivalent alternative;

i. §164.308(a)(7)(ii)(E), which requires assessment of the relative criticality of specific applications and data in support of other contingency plan components, or documentation of why implementation of such procedures were not reasonable or appropriate, and implementation of an equivalent alternative;

j. § 164.308(a)(8), which requires periodic technical and nontechnical evaluations of a covered entity's security policies and procedures;

k. § 164.308(b), which requires that a business associate obtain written assurances from its subcontractor concerning the appropriate safeguarding of ePHI;

l. § 164.312(a)(1), (2)(i), and (2)(iv), which require technical policies and procedures for systems that maintain ePHI to allow access to persons granted access rights, unique user identification, and a mechanism to encrypt ePHI;

m. § 164.312(b), which requires controls for recording and examining activity in systems that contain or use ePHI;

n. § 164.312(d), which requires procedures to verify that a person seeking access to ePHI is the one claimed;

o. § 164.316(b), which requires the implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule;

p. § 164.404, which requires notification of individuals whose unsecured ePHI is accessed as the result of a breach, including a description of the types of unsecured ePHI involved in the breach.

27. Respondents' conduct also violated the Data Breach Notification Law, which requires disclosure of a data breach without unreasonable delay and no later than sixty (60) days from breach discovery. Respondents' conduct also violated the Safeguards Law, which requires anyone in possession of personal information to safeguard such information from misuse, and CUTPA, which prohibits unfair and deceptive business practices.

28. Respondents neither admit nor deny the Attorney General's findings, paragraphs 1-27 above.

29. At the time of the attack, the PJ&A principals included Jeffrey Hubbard, Brittany Larson, and David Campbell.

30. As of the Effective Date, PJ&A, PJ&A Coding, PJ&A Radiology, and MTC are insolvent and inactive.

31. The Attorney General finds the relief and agreements contained in this Assurance appropriate and in the public interest. Therefore, the Attorney General is willing to accept this Assurance pursuant to the above-referenced consumer protection and privacy laws.

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

III. PROSPECTIVE RELIEF

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

a. "Active" shall refer to an entity which meets any one or more of the following criteria:

i. Generates monthly revenue of over $5,000.00;

ii. Has active contracts with a Covered Entity or Business Associate to provide goods or services.

b. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103.

c. "Consumer" shall mean any individual whose PI and/or Protected Health Information is processed, stored, or otherwise made accessible by a Respondent.

d. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103.

e. "Data Breach" shall mean the security event discovered by PJ&A on or about May 2, 2023, and publicly announced on November 3, 2023, in which a malicious cyber-attacker gained unauthorized access to portions of the PJ&A Network that stored PI and/or Personal Health Information.

f. “Effective Date” shall be the execution date of this Assurance.

g. “Encrypt”, “Encrypted” or “Encryption” shall mean encoding data into ciphertext—at rest or in transit—rendering it unusable, unreadable, or indecipherable without converting the ciphertext to plaintext, through the use of a reasonable confidential process and key, leveraging a security technology, methodology, or encryption algorithm commensurate with the sensitivity of the data at issue. The manner of Encryption shall conform to existing industry standard.[2]

h. “Multi-factor 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.

i. “Personal Information” or “PI” shall mean personal information as defined in Connecticut General Statutes § 36a-701b(a)(2) and Connecticut General Statutes § 42-471(c)(1) as of the execution of this Assurance.

j. “PJ&A” shall mean Perry Johnson & Associates, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

k. The “PJ Entities” shall mean PJ&A, Perry Johnson, Inc., Perry Johnson and

[2] For the purposes of this Assurance, the term “existing industry standard” applies to what the standard may become as the industry changes over time. As of the Effective Date, the existing industry standard shall be defined pursuant to Federal Information Processing Standards Publication 140-3.

Associates Coding, Inc., Perry Johnson & Associates Radiology, Inc. and Medical Transcription and Coding, Inc.

l. "PJ Entity" shall mean any one or more of the PJ&A Entities, or any later-created entity controlled by a PJ Owner that is a Covered Entity or Business Associate.

m. The "PJ Owners" shall mean all shareholders owning more than 5% of any PJ Entity, including but not limited to Perry L. Johnson, an individual.

n. "PJ Network" shall mean all networking equipment, technical infrastructure relating to on-premises, cloud-based, and/or colo-databases or data stores, applications, servers, and endpoints that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned, operated, and/or controlled by or on behalf of PJ&A or a PJ Entity; and (c) process, store, or have access to PI and/or Protected Health Information of Consumers who reside in the United States.

o. "PJI" shall refer to Perry Johnson, Inc. and its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States

p. "Protected Health Information" or "PHI" shall be defined in accordance with 45 C.F.R. § 160.103, including electronic protected health information.

q. "Security Incident" shall mean any compromise, or imminent threat of a compromise to the confidentiality, integrity, or availability of PI or PHI stored within, accessed, or transmitted through a PJ Network, by unauthorized access

or inadvertent disclosure, including but not limited to an incident for which notification may be required under Connecticut's data breach notification law or HIPAA. For purposes of this definition, "availability" shall not include an intentional limitation on the availability of PI or PHI, such as for purposes of performing maintenance on a PJ Network.

A. *GENERAL COMPLIANCE*

33. Each PJ Entity shall comply with the Connecticut Consumer Protection Law, the Connecticut Safeguards Law, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D in connection with the collection, use, and maintenance of PHI.

34. Each PJ Entity that is not Active shall, within ten (10) business days of the date the PJ Entity is no longer required to retain PI or PHI for ongoing business or applicable legal reasons, promptly return or destroy, and require the return or destruction of, all PI and PHI maintained by or on behalf of the PJ Entity.

35. Respondents will not hire, employ, or otherwise engage any person who served as a President, Treasurer, Secretary, or Director of PJ&A, or any person who had primary responsibility for managing privacy, information security, or HIPAA compliance, at the time of the incident, or for five years before the incident, for any role which would grant them direct or indirect responsibility for managing privacy, information security, or HIPAA compliance.

36. Respondents and the PJ Owners shall give written notice to the Attorney General sixty (60) days prior to the occurrence of any of the following:

a. A PJ Entity that is not Active becomes Active;

b. A merger, acquisition, or other change of control of a PJ Entity; or

c. A PJ Owner incorporates, acquires, or gains an ownership interest of more than 15% in any Covered Entity or Business Associate.

B. *REQUIREMENTS FOR ACTIVE PJ ENTITIES*

37. PJI, and every PJ&A Entity on the first business day after it becomes Active, shall abide by paragraphs 38 through 59 of this Assurance.

C. *INFORMATION SECURITY PROGRAM*

38. Each Active PJ Entity that collects, stores, transmits, destroys, and/or maintains PI or PHI shall maintain a comprehensive Information Security Program that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI. The Information Security Program shall include the specific information security safeguards set forth in Paragraphs 41 through 55 of this Assurance, provided, however, that an Active PJ Entity which does not collect, store, transmit, destroy, or maintain PHI shall not be required to adopt safeguards that are specific to PHI. The Information Security Program shall adopt, where feasible, principles of zero trust architecture. The Active PJ Entity 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 PI and PHI;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks the Active PJ

Entity identified that are appropriate to: (i) the size and complexity of the Active PJ Entity's operations; (ii) the nature and scope of the Active PJ Entity's activities; and (iii) the volume and sensitivity of the PI and PHI that the Active PJ Entity collects, stores, transmits, and/or maintains.

c. Assess and document, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks the Active PJ Entity identified in (a) above, 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 PI and PHI, contractually require service providers to implement and maintain appropriate safeguards to protect PI and PHI, and take appropriate steps to verify service providers are complying with the contractual requirements;

f. If the Active PJ Entity creates, receives, maintains, or transmits PHI, require business associate agreements consistent with the requirements of 45 C.F.R. § 164.504(e)(1); and

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

of the Program.

39. Each Active PJ Entity shall designate a qualified person to be responsible for implementing, maintaining, and monitoring the Information Security Program. The designated individual shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of the individual's role in implementing, maintaining, and monitoring the Information Security Program. The designated individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management, and shall report at a minimum semi-annually to the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning the Active PJ Entity's Information Security Program. Such reports shall be in writing and include, but not be limited to, the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by the Active PJ Entity, and any barriers to the success of the Information Security Program.

40. Each Active PJ Entity shall provide notice of the requirements of the 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 Active PJ Entity shall provide role appropriate security awareness and privacy training to all personnel whose job involves access to or responsibility for PI and PHI. The notice and training required under this paragraph shall be provided to the appropriate employees within ninety (90) days of the effective date of the Assurance, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security

Program or gains access to or responsibility for PI and PHI, whichever occurs later. The Active PJ Entity shall provide such training on at least an annual basis. The Active PJ Entity shall document that it has provided the notices and training required in this paragraph.

D. *PERSONAL INFORMATION SAFEGUARDS AND CONTROLS*

41. Access and Authentication Controls: Each Active PJ Entity shall, to the extent it has not already done so, establish and implement, and thereafter maintain, policies and procedures to appropriately limit access to PI and PHI that the Active PJ Entity collects, stores, transmits, destroys, and/or maintains. The policies and procedures shall require, at a minimum:

a. Granting individuals and organizations access only to those resources and data that are necessary for their business functions; for the avoidance of doubt, this subparagraph includes, but is not limited to, resources and data maintained on the Active PJ Entity's network;

b. Promptly removing individuals' and organizations' access to resources and data upon separation, or, upon an individual's change in responsibilities, promptly removing the individual's access to resources and data that are no longer needed to discharge those responsibilities;

c. Prohibiting the use of shared individual user accounts without individualized authentication from each individual; and

d. Conducting an audit, not less than semi-annually, to ensure compliance with these policies.

42. Account Audit: Within ninety (90) days of the effective date of this Assurance, each

Active PJ Entity shall conduct an audit to ensure compliance with subparagraphs 41(a) and (b).

43. Multi-Factor Authentication: Each Active PJ Entity shall, to the extent it has not already done so, implement, and thereafter maintain multi-factor authentication for all individual user accounts, including system administrator accounts, and for remote access to its computer network.

44. Password Management: Each Active PJ Entity shall establish and implement, and thereafter maintain, policies and procedures requiring the use of strong, complex passwords and password rotation, and ensuring that stored passwords are properly protected from unauthorized access. Such policies and procedures shall prohibit the use of default, shared, or generic passwords.

45. Encryption: Each Active PJ Entity shall encrypt PI and PHI that it collects, stores, transmits, and/or maintains using an encryption method appropriate to the sensitivity of the PI and PHI.

46. Asset Inventory: Each Active PJ Entity shall maintain and regularly update an inventory that appropriately identifies all assets containing PI and PHI.

47. Risk Assessment Program: Each Active PJ Entity shall conduct annual risk assessments, consistent with the requirements of HIPAA, which shall include identification of all reasonably anticipated internal and external risks to the security, confidentiality, or integrity of PI and PHI. Any entity that collects, uses, or maintains PHI shall ensure the assessment is consistent with 45 CFR § 164.308(a)(1)(ii), which requires a risk analysis, and 45 CFR § 164.308(a)(8), which requires a periodic evaluation. The results of the risk assessment shall be documented, and such documentation shall be maintained by the designated individuals referenced in Paragraph 39 of this Assurance and be available for inspection by the third-party assessor described in Paragraph

58 of this Assurance.

48. Penetration Testing: Each Active PJ Entity shall establish and implement, and thereafter maintain, a penetration testing program designed to identify, assess, and remediate security vulnerabilities within the Active PJ Entity's environments. Testing shall occur on at least an annual basis. The results of the testing, assessment, and remediation shall be documented, and such document shall be maintained by the designated individual referenced in Paragraph 39 of this Assurance and be available for inspection by the third-party assessor described in Paragraph 58 of this Assurance.

49. Segmentation: Each Active PJ Entity shall, to the extent it has not already done so, establish and implement, and thereafter maintain, policies and procedures designed to properly segment its network and ensure that communication between partitions is permitted only to the extent necessary to meet business and/or operational needs. This includes, but is not limited to, designating specific partitions for storing PI and PHI as well as creating clear boundaries between partitions that contain PI and/or PHI and those that do not.

50. Data Loss/Exfiltration Prevention: Each Active PJ Entity shall implement, and thereafter maintain, a reasonable data loss prevention technology to detect and prevent unauthorized data exfiltration from its networks.

51. Monitoring and Logging: Each Active PJ Entity shall implement, and thereafter maintain, controls to log and monitor all security and operational activity related to the Active PJ Entity's networks, systems, and assets. The controls shall, at a minimum: (i) provide for centralized logging that includes collection and aggregation of logging for the Active PJ Entity's network and any platforms or applications operated by or on behalf of the Active PJ Entity that

collect, use, store, retrieve, transmit, display, maintain, or otherwise process PI and PHI, and (ii) use automated processes to monitor for and alert security personnel to anomalous activity. The Active PJ Entity shall also establish and maintain policies and procedures to regularly review appropriate records for anomalous activity. The Active PJ Entity shall store logs of events that indicate anomalous activity for a period of time that is sufficient to detect, investigate, and respond to security incidents.

52. Intrusion Detection and Prevention (IDS/IPS) Solution: Each Active PJ Entity shall implement, and thereafter maintain, reasonable intrusion detection and prevention (IDS/IPS) systems designed to detect and prevent unauthorized access to its environment.

53. Endpoint Detection and Response (EDR) Solution: Each Active PJ Entity shall, to the extent it has not already done so, implement, and thereafter maintain, current, up-to-date endpoint detection and response (EDR) solutions or software on its networks, which shall be at the highest technical level available.

E. *POLICIES*

54. Each Active PJ Entity shall establish and implement, and thereafter maintain, reasonable written policies and procedures that govern asset management, identity and access management, encryption, risk management, network management, and vulnerability management.

55. Each Active PJ Entity shall establish and implement, and thereafter maintain, policies and procedures governing its collection, use, retention, and disposal of PI and PHI. The PJ&A Entity shall securely dispose of PI and PHI when there is no business or legal reason to retain such PI and PHI. In particular, these policies and procedures shall:

a. identify responsible team members for accountability;

b. define the applicable data;

c. identify clear disposal requirements and criteria;

d. identify the areas where PI and/or PHI data may be stored;

e. identify data retention standards for such files; and

f. identify related and dependent processes.

F. *INCIDENT RESPONSE*

56. Each Active PJ Entity shall establish and implement, and thereafter maintain, a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following:

a. If the Active PJ Entity has reason to believe a Security Incident has occurred, the Active PJ Entity shall promptly conduct a reasonable investigation to determine, at a minimum, whether PI and PHI was accessed or acquired without authorization, and, if so, what PI and PHI was accessed or acquired.

b. If the Active PJ Entity determines PI and PHI has been, or is reasonably likely to have been, accessed or acquired without authorization, the Active PJ Entity shall expediently provide each Consumer whose PI or PHI has been, or is reasonably believed to have been, accessed or acquired without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the Security Incident that is reasonably individualized to the customer including, at a minimum, the timing of the Security Incident, whether the Consumer's PI or PHI was accessed or acquired without authorization, what PI or PHI was accessed or acquired,

and what actions have been taken to protect the Consumer.

57. If a Security Incident occurs, the PJ Entity shall create a report that includes a description of the Security Incident and the PJ Entity's response to that Security Incident ("Security Incident Report"). The Security Incident Report shall be made available for inspection by the Third-Party Assessor as described in Paragraph 58.

G. *INFORMATION SECURITY PROGRAM ASSESSMENTS*

58. Within ninety (90) days of becoming Active, each Active PJ Entity shall obtain a comprehensive assessment of the information security of the Active PJ Entity's networks conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Assessment Report") and provided to the Attorney General within two weeks of completion. Annually for three (3) years thereafter, the Active PJ Entity shall obtain Third-Party Assessment Reports which the Active PJ Entity shall maintain for six (6) years from the date of each Third-Party Assessment Report and shall provide to the Attorney General upon request. The third-party assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA), or a similarly qualified person or organization; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security. The Third-Party Assessment Reports shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by the Active PJ Entity's Information Security Program;

b. Document the extent to which the identified administrative, technical, and

physical safeguards are appropriate considering the Active PJ Entity's size and complexity, the nature and scope of the Active PJ Entity's activities, the sensitivity of the PI and PHI maintained on the networks and the reasonably anticipated risks;

c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by the Active PJ Entity meet the requirements of the Information Security Program and the Assurance; and

d. Make recommendations to enhance data security measures.

H. *ACCOUNTING*

59. Each Active PJ Entity shall observe and implement an Income Tax Basis of Accounting.

I. *ACCESS TO RECORDS*

60. Respondents shall retain the documentation and reports required by paragraphs 38 through 58 for at least six years. Such documentation and reports shall be made available to the Attorney General within fourteen (14) days of a written request from the Attorney General. The documentation and reports required by paragraphs 38 through 58 may not be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any other claim.

IV. MONETARY RELIEF

61. Respondents shall pay to the Attorneys General ten million dollars ($10,000,000) in penalties and costs as follows:

a. A payment of three hundred thousand dollars ($300,000) shall be paid in full

within fourteen (14) days of the Effective Date of this Assurance;

b. Nine million seven hundred thousand dollars ($9,700,000) shall be suspended, provided however, that the suspended amount will be immediately due and payable if the Attorney General finds that representations Respondents have provided to the Attorney General concerning their finances are not materially accurate or if Respondents (or their successors) violate the terms of this Assurance.

c. The Attorney General's agreement to suspend nine million seven hundred thousand dollars ($9,700,000) is expressly premised upon the truthfulness, accuracy, and completeness of Respondents' representations concerning their inability to pay the amount in its entirety due to certain Respondents' insolvency and their ability to comply with the terms of this Assurance.

62. Said payments shall be divided and paid by Respondents directly to each of the Attorneys General in an amount designated by the Attorneys General. Payment shall be made in accordance with instructions provided to the Respondents by the Attorneys General. **Of the total amount, Respondents shall pay $2,222,222.00 to the Connecticut Attorney General, of which $2,155,556.00 shall be suspended and $66,666.00 shall be paid in full in accordance with Paragraph 61 of this Assurance**. Said payment shall be used by the Connecticut Attorney General for such purposes that may include, but are not limited to, being placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid/ restitution fund or revolving fund, used to defray costs of the inquiry leading hereto, or for attorneys' fees and other costs of

investigation, or for other uses permitted by state law, at the sole discretion of the Connecticut Attorney General.

V. NOTICE AND WRITTEN RESPONSE

63. If the Attorney General believes a Respondent has failed to comply with a provision of the Assurance, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of the citizens of Connecticut or create an emergency requiring immediate action, prior to taking legal action for any alleged failure to comply with the Assurance, the Attorney General shall provide notice to Respondent of such failure to comply. Respondent shall have 14 days from receipt of such notice (the "Notice Period") to provide a written response, including either a statement that Respondent believes it is in full compliance with the relevant provision or a statement explaining why it did not comply with the relevant provision, how it has come into compliance or when it will come into compliance, and the actions it has taken to prevent future violations. Respondents shall not seek a declaratory judgment concerning any alleged failure to comply with the Assurance during the Notice Period.

VI. MISCELLANEOUS

64. Respondents expressly agree and acknowledge that the Attorney General 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 agree and acknowledges that in the event the Assurance is voided pursuant to paragraph 71:

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

b. the Attorney General may use statements, documents or other materials produced

or provided by Respondents prior to or after the effective date of this Assurance; and

c. any civil action or proceeding must be adjudicated by the courts of the State of Connecticut, and that Respondents irrevocably and unconditionally waive any objection based upon personal jurisdiction, inconvenient forum, or venue.

65. If a court of competent jurisdiction determines that a Respondent has violated the Assurance, the Respondent shall pay to the Attorney General 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. This Assurance is not intended, and should not be construed, as an admission of liability by Respondents.

67. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondents. Respondents shall include in 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 Attorney General. Notwithstanding the forgoing, nothing herein waives or limits any immunity, supremacy or other authority applicable or assertable by or on behalf of the federal government or any agency thereof.

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

69. Any failure by the Attorney General to insist upon the strict performance by a Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the Attorney General, 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 Respondent.

70. All notices, reports, requests, and other communications pursuant to this Assurance 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 Respondent Perry Johnson & Associates, Inc., to:

Martin Van Brauman
President
Perry Johnson & Associates, Inc.
1489 W. Warm Springs Road, Suite 110
Henderson, NV 89012

If to Respondent Perry Johnson, Inc., to:

Martin Van Brauman
President
Perry Johnson, Inc.
755 W. Big Beaver Road, Suite 1300
Troy, MI 48084

If to Respondent Perry Johnson & Associates Coding, Inc., to:

Martin Van Brauman
Director
Perry Johnson & Associates Coding, Inc.
8275 S. Eastern Avenue, Suite 200-535
Las Vegas, NV 89123

If to Respondent Perry Johnson & Associates Radiology, Inc., to:

Martin Van Brauman
General Counsel
Perry Johnson & Associates Radiology, Inc.
1515 North Federal Highway, Suite 300
Boca Raton, FL 33432

If to Respondent Medical Transcription and Coding, Inc., to:

Martin Van Brauman
General Counsel
Medical Transcription and Coding, Inc.
1489 W. Warm Springs Road, Suite 110
Henderson, NV 89012

If to the Connecticut Attorney General, to:

Michele S. Lucan, Chief of the Privacy Section
Office of the Attorney General
Privacy and Data Security Section
165 Capitol Avenue
Hartford, CT 06106
michele.lucan@ct.gov
kileigh.nassau@ct.gov

71. The Attorney General has agreed to the terms of this Assurance based on, among other things, the representations made to the Attorney General by Respondents and their counsel and the Attorney General's own factual investigation as set forth in the Findings, paragraphs 1-28 above. Respondents represent and warrant that neither they nor their counsel have made any material representations to the Attorney General that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or misleading, this Assurance is voidable by the Attorney General in the Attorney General's 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 Respondents in agreeing to this

Assurance.

73. The obligations of this Assurance set forth in paragraphs 41-53 shall expire at the conclusion of the seven (7) year period after the Effective Date.

74. Respondents represent and warrant, through the signature below, that the terms and conditions of this Assurance are duly approved.

75. Respondents agree not to take any action or to make or permit to be made any public statement denying, directly or indirectly, the propriety of this Assurance or the Attorney General's investigation. Nothing in this paragraph affects Respondents' right to take legal or factual positions in defense of litigation or other legal proceedings to which the Attorney General is not a party.

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

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

78. 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 Attorney General, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

79. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

80. This Assurance shall be governed by the laws of Connecticut without regard to any conflict of laws principles.

81. 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.

82. 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.

FOR THE RESPONDENTS

PERRY JOHNSON & ASSOCIATES, INC.

By: _____
Martin Van Brauman
General Counsel
Perry Johnson & Associates, Inc.
1489 W. Warm Springs Road, Suite 110
Henderson, NV 89012

PERRY JOHNSON, INC.

By: _____
Martin Van Brauman
General Counsel
Perry Johnson, Inc.
755 W. Big Beaver Road, Suite 1300
Troy, MI 48084

PERRY JOHNSON & ASSOCIATES CODING, INC.

By: _____
Martin Van Brauman
General Counsel
Perry Johnson & Associates Coding, Inc.
8275 S. Eastern Avenue, Suite 200-535
Las Vegas, NV 89123

PERRY JOHNSON & ASSOCIATES RADIOLOGY, INC.

By: _____
Martin Van Brauman
General Counsel
Perry Johnson & Associates Radiology, Inc.
1515 North Federal Highway, Suite 300
Boca Raton, FL 33432

MEDICAL TRANSCRIPTION AND CODING, INC.

By: _____
Martin Van Brauman
General Counsel
Medical Transcription and Coding, Inc.
1489 W. Warm Springs Road, Suite 110
Henderson, NV 89012

FOR THE STATE OF CONNECTICUT

Accepted by:

WILLIAM TONG
Connecticut Attorney General

By: _____ Date: __11/6/26_____

Michele S. Lucan
Deputy Associate Attorney General/ Chief
Privacy and Data Security Section
Office of the Attorney General
165 Capitol Avenue
Hartford, Connecticut 06106

FOR THE DEPARTMENT OF CONSUMER PROTECTION

Accepted by:

BRYAN CAFFERELLI
Commissioner, Consumer Protection

By: ___ _____ Date: _11/6/26_____
Name:
Title:
Department of Consumer Protection
Legal Division
450 Columbus Boulevard
Hartford, Connecticut 06103