BUSINESS ASSOCIATE AGREEMENT

THIS Business Associate Agreement ("Agreement") dated February 18, 2026, (the "Effective Date"), is entered into by and between Premier Medical Associates of Florida, LLC ("Covered Entity") and [Ocala Fire Rescue] ("Business Associate"), each a "Party" and collectively, the "Parties." Initially capitalized terms, not defined herein, will have the meaning ascribed to them in the Services Agreement, as defined below.

WHEREAS, Covered Entity and Business Associate have entered into, are entering into, or may subsequently enter into, written agreements or arrangements (collectively, the "Services Agreement") pursuant to which Business Associate may provide products and/or services for Covered Entity that require Business Associate to access, create and use health information that is protected by state and/or federal law.

WHEREAS, pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health & Human Services ("HHS") promulgated the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards"), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards to protect the privacy of certain individually identifiable health information ("Protected Health Information" or "PHI").

WHEREAS, pursuant to HIPAA, HHS issued the Security Standards (the "Security Standards"), at 45 C.F.R. Parts 160, 162 and 164, for the protection of electronic protected health information ("EPHI").

WHEREAS, in order to protect the privacy and security of PHI, including EPHI, created or maintained by or on behalf of Covered Entity, the Privacy Standards and Security Standards require a Covered Entity to enter into a "business associate agreement" with certain individuals and entities providing services for or on behalf of Covered Entity if such services require the use or disclosure of PHI or EPHI.

WHEREAS, on February 17, 2009, the federal Health Information Technology for Economic and Clinical Health Act was signed into law (the "HITECH Act"), and the HITECH Act imposes certain privacy and security obligations on covered entities in addition to the obligations created by the Privacy Standards and Security Standards.

WHEREAS, the HITECH Act revises many of the requirements of the Privacy Standards and Security Standards concerning the confidentiality of PHI and EPHI, including extending certain HIPAA and HITECH Act requirements directly to business associates.

WHEREAS, the HITECH Act requires that certain of its provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon covered entities as well as business associates.

NOW, THEREFORE, in consideration of the foregoing recitals, the mutual promises and covenants set forth herein and other good and valuable consideration, the receipt and sufficiency of which hereby are acknowledged, the Parties agree as follows:

1. Definitions.

1.1. Breach. "Breach" has the meaning given to such term at 45 C.F.R. § 164.402.

1.2. Discovery. "Discovery" shall mean the first day on which an Incident (as defined herein) is known to Business Associate (including any person that is an employee, officer, or vendor of Business Associate), or should reasonably have been known to Business Associate, to have occurred.

1.3. Incident. "Incident" shall have the meaning provided under Section 2.6.

1.4. Individual. "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).

1.5. Protected Health Information or PHI. "Protected Health Information" shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. §160.103, limited to the information created, received, transmitted, or maintained by Business Associate on behalf of or for Covered Entity. For purposes of this Agreement, "Protected Health Information" or "PHI" shall collectively refer to Protected Health Information, Electronic Protected Health Information ("ePHI") as defined in 45 C.F.R. § 160.103, and "Personal Information" as defined below.

1.6. Personal Information. Personal Information ("PI"), also known as "Personally Identifiable Information," "Personal Data," and similar terms, shall have the meaning provided under state law. For purposes of this Agreement, Personal Information shall include any data elements that identify an individual or that could be used to identify an individual, including but not limited to an individual's first name or initial and last name in combination with one or more of the following data elements: social security number; driver's license or state issued identification number; credit or debit card number; medical information (such as an individual's condition, treatment, or payment information); financial information, such as checking account or other account number (either in combination with a required security code, access code, or password that would permit access to the account, or alone if the account does not require such an access code); or other identifying information, such as email addresses and usernames in combination with passwords or security questions, date of birth, mother's maiden name, digital signature, passport number, fingerprint or other biometric data, an insurance policy number, employment information, employment history, an employer, student, tribal, or military identification numbers.

1.7. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

1.8. Security Incident. "Security Incident" shall have the meaning provided in 45 C.F.R. § 164.304.

1.9. Terms used but not otherwise defined in this Agreement shall have the same meaning as given to those terms in the HIPAA Rules. A regulatory reference in this Agreement means the section as in effect or as amended, and for which compliance is required.

2. Business Associate's Obligations.

2.1. Permitted Use and Disclosure of PHI. Business Associate shall use and disclose PHI only as permitted by this Agreement or as required by law. To the extent that Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Rules, Business Associate shall comply with the provisions in the HIPAA Rules that would apply to Covered Entity in the performance of such obligation(s). Business Associate is only permitted to:

2.1.1. Use or disclose PHI to perform its obligations and functions under the Agreement, provided that Business Associate shall not use or disclose PHI in any manner that would constitute a violation of the HIPAA Rules if done by Covered Entity;

2.1.2. Use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities;

2.1.3. Disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is Required By Law, or if Business Associate obtains (i) reasonable written assurances from the recipient that the recipient will keep the PHI confidential, and will use or further disclose the PHI only as Required By Law or for the purpose for which it was disclosed to the recipient, and (ii) a written agreement from such third party to immediately notify Business Associate of any instance of which the recipient is aware in which the confidentiality of the PHI has been breached; and

2.1.4. Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B) to the extent specified in the Agreement.

2.2. Safeguards. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that Business Associate creates, receives, maintains, uses, discloses, or transmits on behalf of Covered Entity, as required by the HIPAA Rules. Business Associate shall comply with the requirements in 45 C.F.R. Part 164, subpart C. In addition, Business Associate shall remain familiar with current threats to PHI as they evolve and reasonably and appropriately take steps to mitigate those threats. Business Associate shall comply with all applicable international, federal, state and local laws, statutes, acts, rules and regulations, including the Information Security Requirements attached hereto as Attachment 1.

2.3. Minimum Necessary. Business Associate, and its agents and subcontractors, shall request, use and disclose only the minimum necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure (as described in 45 C.F.R. § 164.502(b) and § 164.514(d)). To the extent practicable, all uses and disclosures must be restricted to information in a Limited Data Set (as described in 45 C.F.R. § 164.514(e)(2)).

2.4. Prohibited Uses and Disclosures. Business Associate shall not use or disclose PHI for any purpose other than as specifically permitted by this Agreement. Specifically, but without limitation, Business Associate (a) shall not use or disclose PHI for fundraising or marketing purposes, (b) shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested a special restriction on disclosure and has paid out of pocket in full for the health care item or services to which the PHI solely relates, and (c) shall not directly or indirectly receive remuneration in exchange for PHI (except if submission of PHI to Covered Entity is necessary for Covered Entity to pay Business Associate for performing services under the Agreement, or with Covered Entity's consent and as permitted by 42 U.S.C. § 17935(d)(2)).

2.5. Agents & Vendors. Business Associate agrees to ensure that any agent or subcontractor to whom it provides PHI agrees in writing to the same restrictions and conditions that apply through this Agreement to Business Associate.

2.6. Incident Reporting, Mitigation, and Remediation: Business Associate shall report to Covered Entity any of the following immediately after Discovery by Business Associate or any Vendor: (i) any acquisition, access, use or disclosure of PHI not provided for in this Agreement or the Agreement; (ii) any Security Incident involving PHI; (iii) any Breach of Unsecured PHI; and (iv) any loss, destruction, alteration, or other event in which PHI cannot be accounted for (collectively, an "Incident"). Business Associate shall implement reasonable systems for the Discovery and prompt reporting of any Incidents and shall train Business Associate personnel regarding the requirements under this Agreement.

2.6.1. Reporting Requirements. Business Associate shall report the information described below to Covered Entity immediately following Discovery of an Incident:

2.6.1.1. the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, disclosed, lost, altered, destroyed, or otherwise unaccounted for:

2.6.1.2. the date of the Incident;

2.6.1.3. the date of the Discovery of the Incident;

2.6.1.4. a description of the types of PHI that were involved; and

2.6.1.5. any other details reasonably requested by Covered Entity.

2.6.2. Risk Assessment. In the event of an Incident, Business Associate shall assist Covered Entity in performing (or at Covered Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised, consistent with and in coordination with any investigation that Covered Entity undertakes. To enable Covered Entity to make a determination whether or not there is a low probability that PHI has been compromised, Business Associate, and any Vendor of Business Associate, shall promptly undertake a risk assessment in coordination with Covered Entity that addresses the following factors and provide the results of such risk assessment to Covered Entity:

2.6.2.1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2.6.2.2. whether the PHI was actually acquired or viewed;

2.6.2.3. the unauthorized person who used the PHI or to whom the disclosure was made; and

2.6.2.4. the extent to which the risk to the PHI has been mitigated.

2.6.3. Breach Determination & Notification. Covered Entity shall make the ultimate determination, in its sole discretion, whether there has been a Breach and if so, whether the required notifications, including to Individuals, third parties, the media, and regulators (such as the Secretary and state regulators), will be provided by Covered Entity or Business Associate. In the event that Covered Entity requires that Business Associate provide such notifications regarding a Breach, any such notices must be approved, in advance, by Covered Entity. Covered Entity's approval shall also be required for the manner of delivering notice of a Breach.

2.6.4. Record Requirements. Business Associate shall maintain complete records regarding any Incident for the period required by 45 C.F.R. § 164.530(j) or such longer period Required By Law, and shall make such records available to Covered Entity promptly upon request, but in no event later than within five (5) business days.

2.6.5. Mitigation & Remediation. Business Associate shall mitigate, to the extent practicable and at its cost, any harmful effects from any Incident (including steps to protect the operating environment). Business Associate also shall take prompt steps designed to prevent the recurrence of any Incident, including any action required by applicable federal and state laws and regulations. All such efforts shall be subject to the Covered Entity's prior written approval. Business Associate must document a corrective action plan, including information on measures that were taken to halt and/or contain the Incident, and provide such documentation to Covered Entity immediately upon request. Business Associate must comply with this provision regardless of any actions taken by Covered Entity.

2.6.6. Ongoing Assistance. Business Associate shall make itself and any employees, subcontractors, or agents assisting Business Associate in the performance of its obligations available to Covered Entity at no cost to Covered Entity to testify as witnesses, or otherwise, in the event of an Incident that results in litigation or administrative proceedings against Covered Entity, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy or arising out of this Agreement.

2.7. Identification of Employees. Business Associate shall maintain a current list of its employees, agents, and Vendors with access to PHI provided by Covered Entity. Upon request, Business Associate shall provide such list to Covered Entity within a reasonable amount of time.

2.8. Access to PHI. To the extent that Business Associate possesses an applicable Designated Record Set, and within a reasonable amount of time (but not to exceed five (5) days) of receipt of a request from Covered Entity to access such PHI, Business Associate shall transmit such information to Covered Entity. If an Individual requests access to PHI directly from Business Associate, Business Associate will forward such a request in writing to Covered Entity within a reasonable amount of time (but not to exceed five (5) days). Covered Entity will be responsible for making all determinations regarding the granting or denial of an Individual's request, and Business Associate shall make no such determinations. If Business Associate maintains PHI in electronic form, Business Associate shall provide such information in electronic format to Covered Entity if requested.

2.9. Amendment of PHI. To the extent that Business Associate possesses an applicable Designated Record Set, Business Associate agrees to make any amendment(s) to PHI that Covered Entity directs or agrees to, pursuant to 45 C.F.R. § 164.526, in the time and manner designated by Covered Entity. Within a reasonable amount of time of receipt of a request by an Individual to Business Associate to amend PHI (but not to exceed five (5) days), Business Associate shall forward to Covered Entity any such requests in writing. Covered Entity shall be responsible for making all determinations regarding amendments to PHI, and Business Associate shall make no such determinations.

2.10. Accounting of Disclosures. Business Associate shall document such disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or Vendors for (6) years prior to the request. In addition, Business Associate agrees that:

2.10.1. Within a reasonable amount of time of receipt of a notice from Covered Entity requesting an accounting of PHI disclosures (but not to exceed five (5) days), Business Associate shall provide Covered Entity with records of such disclosures containing information as outlined in 45 C.F.R. §164.528(b).

2.10.2. Within a reasonable amount of time of receipt of a request by an Individual to Business Associate for an accounting of disclosures of PHI (but not to exceed five (5) days), Business Associate shall forward to Covered Entity any such requests in writing. Covered Entity shall be responsible for providing an accounting of PHI disclosures to the Individual. Business Associate will not provide an accounting of its disclosures directly to the Individual.

2.11. Government Access. Upon request, Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to Covered Entity and to the Secretary to the extent required for determining Covered Entity's compliance with the HIPAA Rules. Business Associate shall concurrently provide Covered Entity with a copy of any PHI that Business Associate provides pursuant to any governmental inquiry.

2.12. Indemnification. Business Associate ("Indemnitor"), at its own expense, agrees to defend, indemnify and hold harmless Covered Entity and any of Covered Entity's affiliates, subsidiaries, directors,

officers, employees, representatives, and agents ("Indemnitee") from and against any claim, demand, cause of action, class action, cross-claim, arbitration, judgment, liability, damage, fines, penalties, public relations expenses, government investigation or inquiry, remediation and mitigation efforts regardless of whether required by law (including but not limited to notification letters, credit monitoring services, identity theft insurance, reimbursement for credit freezes, fraud resolution services, identity restoration services, toll free information services for affected Individuals, and any similar service that entities make available to impacted Individuals in the event of an Incident), and costs and expenses relating thereto (including but not limited to costs and expenses of defense, settlement, adjudication, dismissal, expert fees, court costs, investigation expenses, discovery costs, time of Indemnitee personnel, and reasonable attorneys' fees, costs and disbursements of legal counsel) arising from, related to, or in connection with any Incident involving PHI in Indemnitor's possession, custody, or control, or any other breach of this Agreement. Indemnitor's liability under this Agreement shall include direct, indirect, incidental, or consequential, exemplary, punitive, or special damages of any kind or nature whatsoever. This indemnity shall not be construed to limit Indemnitee's rights, if any, to common law indemnity.

The obligations of Indemnitor under this Agreement to defend, indemnify and hold harmless Indemnitee shall be subject to the following: (a) the Indemnitee shall provide the Indemnitor with prompt notice of the claim giving rise to such obligation; provided, however, that any failure or delay in giving such notice shall only relieve the Indemnitor of its obligation to defend, indemnify and hold the Indemnitee harmless to the extent it reasonably demonstrates that its defense or settlement of the claim or suit was adversely affected thereby; (b) the Indemnitor shall have control of the defense and of all negotiations for settlement of such claim or suit; provided, however, that the Indemnitee shall select counsel for such defense reasonably acceptable to Indemnitor with such consent not unreasonably withheld, delayed or conditioned and Indemnitor shall not settle any claim unless such settlement completely and forever releases the Indemnitee from all liability with respect to such claim and unless the Indemnitee consents to such settlement in writing (which consent shall not be unreasonably withheld); and (c) the Indemnitee shall cooperate with the Indemnitor in the defense or settlement of any such claim or suit; provided, however, that the Indemnitee shall be reimbursed for all reasonable out-of-pocket expenses incurred in providing any cooperation requested by the Indemnitor. Subject to clause (b) above, the Indemnitee may also participate in the defense of any claim or suit in which the Indemnitee is involved at its own expense.

2.13. State Law. Business Associate shall comply with applicable state law confidentiality, privacy, security, document retention, and breach notification requirements involving PI. Notwithstanding any provision to the contrary, the provisions of this Agreement shall apply equally with respect to PI as they do to PHI; provided, however, that to the extent that state law is more stringent than the HIPAA Rules or the terms of this Agreement, Business Associate agrees to comply with the requirement that provides more privacy and security protection to PI.

2.14. Standard Transactions. To the extent Business Associate conducts Standard Transaction(s) on behalf of Covered Entity, Business Associate shall, without limitation, comply 45 C.F.R. Part 162, and shall not: (a) Change the definition, data condition or use of a data element or segment in a standard; (b) Add any data elements or segments to the maximum defined data set; (c) Use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification(s); or (d) Change the meaning or intent of the standard's implementation specifications.

2.15. Information Regarding Drug or Alcohol Use Disorders. To the extent that Business Associate receives, stores, processes, or otherwise deals with any substance use disorder information, Business Associate agrees that (i) Business Associate is fully bound by the Confidentiality of Substance Use Disorder Patient Records set forth in 42 C.F.R. Part 2, and (ii) if necessary, Business Associate will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the 42 C.F.R. Part 2 regulations. For purpose of this Section all terms shall have the meanings provided in 42 C.F.R. Part 2.

3. Covered Entity's Obligations.

3.1. Notice of Change in Privacy Practices. To the extent known to Covered Entity, Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

3.2. Notice of Change in Permissions. To the extent known to Covered Entity, Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

3.3. Notice of Change in Use. To the extent known to Covered Entity, Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

3.4. Appropriate Requests. Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

4. Term and Termination.

4.1. Term. This Agreement shall become effective on the Effective Date and shall terminate at the time of the termination or expiration of the Agreement, or earlier as provided herein.

4.2. Termination for Cause. If Covered Entity reasonably determines, in its sole discretion, that Business Associate has materially breached this Agreement, Covered Entity may:

4.2.1. Provide Business Associate with thirty (30) days written notice of the alleged material breach and an opportunity to cure the breach, immediately after which time this Agreement and the Agreement under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity shall be automatically terminated if the breach is not cured; or

4.2.2. Immediately terminate the Agreement.

4.3. Effect of Termination. Upon termination or expiration of the Agreement, Business Associate shall, at Covered Entity's option, return to Covered Entity or destroy all PHI in Business Associate's possession, and/or in the possession of any Vendor or agent of Business Associate. Business Associate shall not retain any copies of the PHI. In the event that return or destruction of the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction of the PHI not feasible, and Covered Entity and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. In such case, Business Associate shall extend the protections of this Agreement to such PHI that is not returned or destroyed, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for as long as Business Associate maintains such PHI. If Covered Entity elects destruction of the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

5. Miscellaneous.

5.1. Amendments. The Parties shall amend this Agreement from time to time as is necessary to achieve and maintain compliance with the HIPAA Rules.

5.2. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the HIPAA Rules and relevant state laws.

5.3. Audits, Inspection and Enforcement. Upon request and with reasonable prior notice by Covered Entity, Business Associate and its agents shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI pursuant to this Agreement or for the purpose of determining whether Business Associate is in compliance with its obligations under this Agreement.

5.4. Relationship to Agreements with Covered Entity. In the event that a provision of this Agreement is contrary to a provision of the Agreement (including any inconsistencies in defined or capitalized terms), this Agreement shall control.

5.5. Survival. Business Associate's obligations under Sections 2 and 4.3 of this Agreement shall survive the termination of this Agreement.

5.6. Waiver. No delay or omission by Covered Entity in exercising any right or power under this Agreement shall impair such right or power or be construed to be a waiver thereof. Any decision by Covered Entity not to enforce a breach of this Agreement shall not be construed to be a waiver of any succeeding breach thereof.

5.7. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

5.8. Data Ownership. Business Associate acknowledges that, between the Parties, Covered Entity is the owner of all PHI and/or ePHI that Covered Entity discloses to Business Associate, or that Business Associate receives from, or creates, maintains, transmits, uses, or discloses on behalf of or in the name of, Covered Entity.

5.9. Due Diligence. Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Agreement and is in compliance with the applicable HIPAA Rules and state laws, and that its agents, Vendors, and vendors comply with this Agreement.

5.10. Judicial or Administrative Proceeding. Business Associate shall notify Covered Entity if it is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

COVERED ENTITY

PREMIER MEDICAL ASSOCIATES OF FLORIDA, LLC

Signature: Craig Esquenazi

Name: Craig Esquenazi

Email: Cesquenazi@neuehealth.com

Phone: 9548172035

Date Signed: 03/04/2026

BUSINESS ASSOCIATE

[OCALA FIRE RESCUE]

Signature: DocuSigned by: Peter Lee 5BB28E162F2E4C2...

Title: City Manager

Email: plee@ocalafl.org

Phone:

Date Signed: 4/7/2026

Approved as to form and legality:

Signed by: William E. Sexton, Esq. 4A55AB8A8ED04F3...

William E. Sexton, Esq.

City Attorney

[**SIGNATURE PAGE**]

ATTACHMENT 1

INFORMATION SECURITY REQUIREMENTS

1. Definitions:

All capitalized terms used but not otherwise defined herein, shall have the meanings set forth in the Agreement.

"Covered Entity Data" shall mean all data originating from Covered Entity.

"Data Masking" means the process of replacing live data elements to conceal Covered Entity Data.

"Information Processing System(s)" means the individual and collective electronic, mechanical, or software components of Business Associate operations that store and/or process Covered Entity Data.

"Information Security Event" is an unexplained or unexpected activity that indicates the security of an Business Associate Information Processing System may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

"Non-Production Environment" means the Information Processing Systems used for any purpose other than live use (e.g., development, system testing, pre-production, integration testing, user acceptance testing, performance testing, staging, etc.).

"Personal Information" means any Protected Health Information or PHI, as that term is defined in the Business Associate Agreement entered into between the parties.

"Production Environment" means the Information Processing Systems used to process live Covered Entity Data, employed during the provision of services to Covered Entity.

2. Information Security Program: Business Associate will implement and maintain an information security program that establishes roles and responsibilities for information security and supports the confidentiality, integrity and availability of Information Processing Systems operated by or on behalf of Business Associate.

3. Security Policy: Business Associate will maintain information security policies that define requirements for access control, application and system development, passwords, remote access, data classification, operational security, network security and physical security. The information security policies will be reviewed annually, or when significant changes to the environment occur, to ensure their continuing suitability, adequacy and effectiveness.

4. Security Awareness Training: All new Business Associate employees will be required to complete security awareness training. Thereafter, all Business Associate employees will be subject to annual training.

5. Required Background Checks: Employment background verification checks on all candidates for employment will be carried out in accordance with applicable laws and regulations and appropriate to the classification of the information to which the candidate, if employed, would have access.

6. Asset Inventory: Business Associate will maintain an inventory of Business Associate Information Processing Systems and media containing Covered Entity Data.

7. Acceptable Use: Business Associate will maintain and enforce corporate security policies for the acceptable use of information and assets.

8. Secure Areas: Business Associate will secure all areas that house Information Processing Systems or media containing Covered Entity Data by the use of appropriate physical security controls in order to ensure that only authorized personnel will be allowed access and to prevent damage and interference.

9. Security Perimeter: Access will be controlled and restricted by use of a defined security perimeter, appropriate security barriers, entry controls and authentication controls.

10. Identification: All individuals entering a Business Associate facility that houses Client Data or Personal Information will be required to wear visible identification to identify them as an employee, contractor, or visitor.

11. Visitors: Visitors to Business Associate facilities that house Client Data or Personal Information will be supervised, or cleared for non-escorted access via a verification process.

12. User Access Management: To protect against unauthorized access or misuse of Covered Entity Data residing on Business Associate Information Processing Systems, Business Associate will employ a formal user registration and de-registration procedure for granting and revoking access and access rights to all Business Associate Information Processing Systems for Business Associate employees.

13. Operating System Access Control: To protect against unauthorized access or misuse of Covered Entity Data residing on Business Associate Information Processing Systems, Business Associate will ensure that access to operating systems is controlled by a secure log-on procedure with username and password credentials at a minimum.

14. Vulnerability Management: Business Associate will employ a process for vulnerability management, including:

    a. Regularly scheduled internal and external system and network vulnerability scans conducted;

    b. Annual network and application layer penetration tests conducted;

    c. Secure application source code scanning and analysis review processes; and

    d. A framework for scheduled remediation of findings.

15. Development Processes: Business Associate will incorporate security into the development lifecycle, including:

    a. Restricting access to source code to authorized users who have a direct need to know; and

    b. Employing oversight quality controls and security management of software development.

    c. Security application code reviews need to be conducted on all code prior to moving into production. All high and critical findings need to be mitigated prior to being promoted into production.

    d. PHI data shall not be used in test or development environments. If PHI is necessary in test or development environments, data needs to be masked, encrypted and protected in the same manner as a production environment.

16. Change Management: Business Associate will utilize processes to control changes in Business Associate's technical environment, including:

    a. Use of formal change control procedures to approve and implemented changes; and

    b. Ensuring file integrity in the operating environment is maintained and monitored for approved change.

17. Incident Response Plan: Business Associate will utilize a formally documented Information Security Event and Incident Response Plan that includes: formation of an incident response team, categorization of incidents and responsibility for receiving alerts and investigations.

18. Incident Training: Business Associate will train all workforce and supplier users of Business Associate Information Processing systems how to report any Information Security Events of which they become aware.

19. Termination of Security Events: Business Associate will use commercially reasonable efforts to immediately terminate any Information Security Events. Business Associate will not allow any Information Security Event that it is able to terminate to persist except as required by law, or as deemed reasonably necessary by Business Associate to determine the identity of the perpetrator.

20. Business Continuity Management: Business Associate will maintain commercially reasonable business continuity management procedures ("BCM Procedures") regarding contingency management to alleviate the effects of any business impacting events that may have a material and adverse impact on Business Associate's ability to perform its obligations under this Agreement.

21. Right to audit: Covered Entity retains the right to audit Business Associate for compliance to the IT security requirements dictated in this Agreement. Covered Entity also can request vulnerability and Penetration tests for the in-scope systems. Covered Entity retains the right to review system architecture drawings and vulnerability scans, penetration tests, application code reviews prior to giving permission to go live. All high and critical findings will need to be mitigated prior to having the systems going live.

22. Encryption: All PHI data needs to be encrypted at rest and in transit.

23. Information security event notification: Covered Entity shall be notified within 24 hours regarding any data incident involving Covered Entity's data and/or environment.

24. Third parties with access to Covered Entity's data: Business Associate must evaluate and hold any third-party companies accountable to the same security requirements detailed in this Attachment 1 and amendment.

Certificate Of Completion

Envelope Id: 27CE15C9-FBC9-8F8A-8006-53FD28F84E1C
Status: Completed
Subject: SIGNATURE - Business Associate Agreement - Premier Medical (OFR/260596)
Source Envelope:
Document Pages: 12
Signatures: 2
Certificate Pages: 5
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

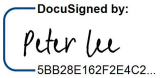
Envelope Originator:
Patricia Lewis
110 SE Watula Avenue
City Hall, Third Floor
Ocala, FL 34471
plewis@ocalafl.org
IP Address: 216.255.240.104

Record Tracking

Status: Original
4/2/2026 11:18:20 AM
Security Appliance Status: Connected

Holder: Patricia Lewis
plewis@ocalafl.org
Pool: StateLocal

Location: DocuSign

Signer Events	Signature	Timestamp
William E. Sexton, Esq. wsexton@ocalafl.gov City Attorney Security Level: Email, Account Authentication (None)	Signed by:  4A55AB8A8ED04F3... Signature Adoption: Pre-selected Style Using IP Address: 216.255.240.104	Sent: 4/2/2026 11:22:12 AM Viewed: 4/2/2026 11:33:30 AM Signed: 4/2/2026 12:23:13 PM
Electronic Record and Signature Disclosure: Accepted: 9/15/2023 9:02:35 AM ID: 313dc6f2-e1d0-44c3-8305-6c087d6cdf0b		
Peter Lee plee@ocalafl.org City Manager City of Ocala Security Level: Email, Account Authentication (None)	DocuSigned by:  5BB28E162F2E4C2... Signature Adoption: Pre-selected Style Using IP Address: 216.255.240.104	Sent: 4/2/2026 12:23:14 PM Viewed: 4/7/2026 9:56:33 AM Signed: 4/7/2026 9:57:02 AM
Electronic Record and Signature Disclosure: Not Offered via Docusign		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	4/2/2026 11:22:12 AM

Envelope Summary Events	Status	Timestamps
Certified Delivered	Security Checked	4/7/2026 9:56:33 AM
Signing Complete	Security Checked	4/7/2026 9:57:02 AM
Completed	Security Checked	4/7/2026 9:57:02 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, City of Ocala - Procurement & Contracting (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact City of Ocala - Procurement & Contracting:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: contracts@ocalafl.org

To advise City of Ocala - Procurement & Contracting of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at contracts@ocalafl.org and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from City of Ocala - Procurement & Contracting

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to contracts@ocalafl.org and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with City of Ocala - Procurement & Contracting

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to contracts@ocalafl.org and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify City of Ocala - Procurement & Contracting as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by City of Ocala - Procurement & Contracting during the course of your relationship with City of Ocala - Procurement & Contracting.