

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is entered into by and between **RESS, Inc.** (d/b/a RES Systems) (“Business Associate”) and _____ (“Covered Entity”) (collectively, “the Parties”) as of the date executed by or on behalf of an authorized representative of Covered Entity (“Effective Date”).

RECITALS

A. The parties have entered into a Services Agreement (the “Services Agreement”) for RESS, Inc.’s Eligibility Lookup Service and/or Managed Care Permanent Placement Notification Service on _____;

B. Under the Services Agreement, Business Associate performs certain services which provide it access to electronic patient health information of Covered Entity;

C. The Parties wish to comply in all respects with the requirements with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), and the 2013 Final HIPAA Omnibus Rule, including all amendments thereto and all rules and regulations promulgated thereunder (collectively, “HIPAA Rules”).

NOW, THEREFORE, the Parties agree as follows:

1. **Definitions.** All capitalized terms used in this BAA but not defined herein shall have the meanings set forth in the HIPAA Rules.

2. **Duties and Responsibilities of Business Associate.**

2.1 *Use and Disclosure of PHI.* Business Associate agrees to not Use or Disclose Protected Health Information (“PHI”) other than as permitted or required by Section 3 of this BAA or as required by law.

2.2 *Safeguards.* Business Associate agrees to use appropriate safeguards and comply with security standards for the protection of Electronic Protected Health Information (“Electronic PHI”) to prevent Use or Disclosure of Electronic PHI other than as provided for by this BAA, pursuant to the Standards for Security of Electronic Protected Health Information in the HIPAA Rules, including those specified in 45 CFR Parts 160 and 164, subparts A and C respectively (collectively, the “Security Rule”). Business Associate further agrees to implement appropriate Administrative, Physical, and Technical Safeguards to protect the confidentiality, integrity and availability of any Electronic PHI in accordance with the HIPAA Rules, including the use of written policies and procedures.

2.3 *Compliance with State and Other Laws.* Business Associate will comply with any applicable federal or state privacy or security law to the extent such law is more protective of Individual privacy than HIPAA Rules, including, but not limited to, the provisions

of the New York State Information Security Breach and Notification Act (General Business Law § 899-aa and State Technology Law, § 208).

2.4 *Reporting.* Business Associate agrees to report to Covered Entity any improper or unauthorized access of PHI, or Use or Disclosure of PHI in violation of this BAA by Business Associate (including, but not limited to, its officers, directors, employees, representatives, subcontractors or agents, or third parties to whom Business Associate disclosed PHI) within two (2) business days of which it becomes aware, and shall provide written notice to Covered Entity without unreasonable delay, and in no event later than ten (10) business days.

2.5 *Mitigation.* Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this BAA or applicable law.

2.6 *Agents.* Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees (or has agreed) to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information. Business Associate agrees to ensure that any agent, including an authorized subcontractor, to whom it provides Electronic PHI, agrees to (or has agreed to) implement reasonable and appropriate Administrative, Physical, and Technical Safeguards to protect such Electronic PHI. If Business Associate discloses PHI to a subcontractor, Business Associate must engage the subcontractor in a written business associate agreement that incorporates the same restrictions and conditions concerning PHI as Business Associate. If Business Associate discloses PHI to an agent, Business Associate must engage the subcontractor in a written business associate agreement that incorporates the same restrictions and conditions concerning PHI as Business Associate.

2.7 *Subcontractors.* Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information as set forth in the Privacy and Security Rules.

2.8 *Right of Access.* Business Associate agrees to provide, within ten (10) business days from the request of Covered Entity, access to, or copies of, PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524,. The provisions of this section shall survive termination of this BAA.

2.9 *Amendments to PHI.* Business Associate agrees to make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity in accordance with HIPAA Privacy Rule standards for amendments of PHI at 45 CFR 164.526, or to take other measures as necessary to satisfy Covered Entity's obligations under the HIPAA Rules.

2.10 *Audit and Inspection.* Upon written request, Business Associate agrees to make internal practices, books, and records relating to the Use and Disclosure of PHI

available to the Secretary in a time and manner reasonably designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA Rules.

2.11 *Accounting of Disclosures.* Business Associate agrees to document any Disclosures of PHI by Business Associate (including by its agents or authorized subcontractors) and information related to such disclosures, that would be required of Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Business Associate agrees to provide to Covered Entity information collected in accordance with this Section promptly, and in any case no later than ten (10) business days after receiving a request by Covered Entity. In the event that a request for an accounting of disclosures is delivered directly to Business Associate, Business Associate shall notify Covered Entity of such request within five (5) business days of receipt thereof. Covered Entity shall determine, in its sole discretion and with the cooperation of Business Associate, whether the accounting will be provided by Business Associate or by Covered Entity to the Individual.

2.12 *Safeguards Against Misuse of PHI.* Business Associate agrees that it will use all appropriate safeguards, in accordance with the Security Rule, including but not limited to the terms set forth in the Security Rule to: (a) reasonably and appropriately protect the confidentiality, integrity, and availability of PHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity; and (b) prevent the Use or Disclosure of PHI other than pursuant to the terms and conditions of this BAA.

2.13 *Additional Privacy and Security Compliance.* To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Rules, Business Associate agrees to comply with the Security Rule as well as the Standards for Privacy of Individually Identifiable Health Information in the HIPAA Rules, including those specified in 45 CFR part 160 and part 164, subparts A and E respectively (collectively, the "Privacy Rule") that apply to the Covered Entity in the performance of such obligation(s). Business Associate acknowledges that pursuant to the HIPAA Rules, the Privacy Rule and Security Rule provisions now apply to Business Associate directly. Such requirements are incorporated by reference as if fully set forth herein.

2.14 *Property Rights in PHI.* Business Associate hereby acknowledges that, as between Business Associate and Covered Entity, all PHI shall be and remain the sole property of Covered Entity, including any forms of PHI developed by Business Associate in the course of fulfilling its obligations under this BAA.

2.15 *Breach Notification.* Effective as of the Compliance Date, Business Associate will comply with Section 13402 of the HITECH Act and the regulations implementing such provisions, currently 45 CFR part 164, subpart D, as such regulations may be in effect from time to time (collectively, the "Breach Notification Rules").

2.15.1 Except as provided in 45 CFR § 164.412, Business Associate will give Covered Entity notice of any Breach of Unsecured PHI promptly, and in any case no later than two (2) business days after the first day on which the Breach is known to Business Associate. Business Associate further agrees to report to Covered Entity, in writing, any Security Incident promptly, and in any case no later than two (2) business days after

confirming such Security Incident relating to Covered Entity's PHI and any remediation or mitigation efforts taken. Business Associate agrees to comply with any subsequent reasonable requests from Covered Entity for Business Associate to notify media or individuals about any Breach, Use or Disclosure, or Security Incident of Covered Entity PHI, as such media notice may be required by law.

2.15.2 The notice required by Business Associate in Section 2.15.1 above shall adhere to the same Content Of Notification standards as set forth in 45 CFR § 164.404(c)(1) and (2). The notice will be in the form of Exhibit A.

2.16 *Covered Entity's Rights of Access and Inspection.* To the extent that PHI may have been conveyed to Business Associate's premises, Covered Entity may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this BAA.

2.17 *Encryption.* Business Associate agrees to secure PHI through the use of encryption and/or destruction as required by Covered Entity's procedure for its internal information systems, including on portable devices and removable media. The Business Associate agrees to encrypt PHI transmitted by the Business Associate to the Covered Entity over a public network.

Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and its employees, agents or representatives available to Covered Entity to testify as witnesses, for document production, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity (including against their respective members, trustees, officers, agents or employees) based upon claimed violation of the HIPAA Rules or other laws relating to security and privacy, except where Business Associate is a named adverse party.

3. **Permitted Uses and Disclosures of Business Associate.**

3.1 *Performance of Services.* Business Associate may Use or Disclose PHI as necessary to perform the functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Services Agreement if (i) such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity or (ii) such use or disclosure is expressly permitted under this Section 3.

3.2 *Minimum Necessary.* Upon Business Associate's use or disclosure of PHI or upon its request of PHI from Covered Entity, Business Associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

3.3 *Proper Management and Administration.* Business Associate may Use or Disclose PHI for the proper management and administration of Business Associate in connection with the performance of services as permitted by this BAA; provided, however, that for any disclosure pursuant to this paragraph Business Associate obtains (i) reasonable assurances from the person or entity to whom the information is disclosed that it will remain confidential and Used or further Disclosed only as required by law or for the purpose for which it

was disclosed to the person or entity, and (ii) the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.4 *Additional Restrictions.* If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the Uses or Disclosures of PHI pursuant to the HIPAA Rules, Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions.

3.5 *Disclosures Required by Law.* If Business Associate believes it has a legal obligation to disclose any PHI, it will notify Covered Entity promptly, and in any case no later than ten (10) business days prior to the proposed release, as to the legal requirement pursuant to which it believes the PHI must be released. If Covered Entity objects to the release of such PHI, Business Associate will allow Covered Entity to exercise any legal rights or remedies Covered Entity might have to object to the release of the PHI, and Business Associate agrees to provide such assistance to Covered Entity, at Covered Entity's expense, as Covered Entity may reasonably request in connection therewith.

4. **Obligations of Covered Entity.**

4.1 Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI. Business Associate will give timely effect to such limitations.

4.2 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. Business Associate will give timely effect to such changes or revocations.

4.3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI. Business Associate will give timely effect to such restrictions.

4.4 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except as specifically allowed by Section 3 of this BAA.

5. **Term and Termination.**

5.1 *Term.* The Term of this BAA shall commence as of the Effective Date and shall terminate when the Services Agreement terminates or at such later date that Business Associate ceases to provide the services set forth in the Services Agreement.

5.2 *Effect of Termination.* Upon termination of this BAA, for any reason, Business Associate shall return or destroy all PHI and Electronic PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, or otherwise in Business Associate's possession. Business Associate shall retain no copies of the

PHI or Electronic PHI in any form. In the event that Business Associate determines that returning or destroying the PHI or Electronic PHI is infeasible, Business Associate agrees to continue to use appropriate safeguards and comply with the security standards for the protection of Electronic PHI pursuant to the Security Rule to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information, and to limit any further Uses and Disclosures of such PHI to only those purposes that make the return or destruction infeasible. This Section 5.2 shall survive the termination of this BAA.

5.3 *Termination of Services Agreement.* The Covered Entity may, at its sole discretion, terminate the Services Agreement, effective immediately, if (i) the Business Associate is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of the HIPAA Rules is made in any administrative or civil proceeding in which the Business Associate has been joined, or (iii) the Business Associate makes a disclosure of PHI in violation of this BAA.

6. **Miscellaneous.**

6.1 *Regulatory References.* A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended, and for which compliance is required.

6.2 *Interpretation.* Any ambiguity in this BAA shall be resolved in favor of a meaning that permits the Parties to comply with HIPAA Rules.

6.3 *Amendment to Agreement.* The parties agree to take such action as is necessary to amend this BAA from time to time in order to comply with the requirements of HIPAA Rules. Any and all amendments to this BAA shall be in writing and signed by both parties. Notwithstanding the foregoing, if any modification to this BAA is required by law or if Covered Entity determines, in its sole discretion, that this BAA must be amended due to a change in applicable federal or state law, Covered Entity shall notify Business Associate of such proposed modification(s) and the parties shall negotiate in good faith an amendment to this BAA. If the parties are unable to mutually agree upon an amendment to this BAA, either party may terminate this BAA and the Master Services Agreement upon the sooner of the compliance date of any change in applicable federal or state law, or sixty (60) days notice.

6.4 *Equitable Relief.* Business Associate agrees that the remedies at law for its breach of this BAA may be inadequate and that monetary damages resulting from such breach may not be readily measured. Accordingly, in the event of a breach or threatened breach by Business Associate of its obligations under this BAA, Covered Entity shall be entitled to immediate injunctive relief and may pursue any other remedies that may be available at law.

6.5 *Training of Business Associate's Employees.* Business Associate represents and warrants to Covered Entity that Business Associate's employees, agents, representatives, and subcontractors who will have access to PHI will (i) receive general training and education and annual refresher training related to the HIPAA Rules, (ii) be familiar with and receive training related to state and federal data breach notification laws and requirements, and

(iii) have specific knowledge of Business Associate's responsibilities and contractual requirements to Covered Entity under the HIPAA Rules (and including applicable state law), in each case prior to being allowed to have access to Covered Entity's PHI.

6.6 *Notice of Request or Subpoena for Data.* Business Associate agrees to notify Covered Entity promptly, but no later than five (5) business days after Business Associate's receipt of any request or subpoena for PHI or an accounting thereof. Business Associate shall promptly comply with Covered Entity's instructions for responding to any such request or subpoena, unless such Covered Entity instructions would prejudice Business Associate. To the extent that Covered Entity decides to assume responsibility for challenging the validity of such request, Business Associate agrees to reasonably cooperate with Covered Entity in such challenge. The provisions of this Section shall survive the termination of this BAA.

6.7 *Third Party Beneficiaries.* This BAA does not create any third party beneficiary rights, except as otherwise expressly noted herein.

6.8 *Notices.* Whenever this BAA requires one party to give notice to the other, such notice shall be addressed as set forth in the Services Agreement, and shall be deemed given: three (3) calendar days after deposit in United States mail, postage prepaid; one (1) calendar day after deposit with a nationally recognized overnight carrier; or upon actual delivery, if delivered by hand.

6.9 *Counterparts.* This BAA may be executed in counterparts, each of which when executed shall be deemed to be an original, and all of which taken together shall constitute one and the same agreement. Signatures on this BAA that are transmitted by telecopy or other electronic means shall be deemed to be the same as a manually executed counterpart for purposes of this BAA.

6.10 *Entire Agreement.* This BAA constitutes the entire agreement between the parties and supersedes all prior negotiations, discussions, representations, or proposals, whether oral or written, unless expressly incorporated or referenced herein, related to the subject matter of this BAA. Unless otherwise expressly provided herein, this BAA may not be modified except in writing signed by the duly authorized representatives of the Parties. If any provision or part thereof is found to be invalid, the remaining provisions shall remain in full force and effect.

6.11 *Successors and Assigns.* This BAA will inure to the benefit of and be binding upon the successors and assigns of the parties. However, this BAA is not assignable by any party without the prior written consent of the other parties.

[signature page follows]

IN WITNESS WHEREOF, the Parties have caused this BAA to be signed and delivered by their duly authorized representatives as of the Effective Date.

COVERED ENTITY:

BUSINESS ASSOCIATE:

_____ RESS, INC.

By: _____

By: _____

Signature

Name: _____

Print Name

Title: _____

Print Title

EXHIBIT A - NOTIFICATION FORM

BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

This notification is made pursuant to the Business Associate Agreement between:

- _____ (Business Associate) and
- _____ (Covered Entity).

The Business Associate hereby notifies _____ that there has been a breach of unsecured (unencrypted) Protected Health Information (PHI) that the Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Description of the breach: _____

Date of the breach: _____

Date of the discovery of the breach: _____

Number of individuals affected by the breach: _____

The types of unsecured PHI that were involved in the breach, such as account number, disability code, full name, address, zip code, date of birth, SSN, drivers license number, credit card / bank account number, claims information, diagnosis/conditions, medications, lab results, other demographic, financial or clinical information: _____

Type of Breach – Specify whether theft, loss, improper disposal, unauthorized access, hacking / IT incident, other (describe), or unknown: _____

Location of Breached Information – Specify whether laptop, desktop computer, network server, email, other portable electronic device, electronic medical record, paper, or other (describe): _____

Safeguards in Place Prior to the Breach – such as firewalls, packet filtering (router-based), secure browser sessions, strong authentication, encrypted wireless, physical security, logical access control, anti-virus software, intrusion detection, biometrics, other (please specify):

Description of what the Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches:

Description of any steps that individuals should take to protect themselves from potential harm resulting from the breach:

Form completed by:

Name: _____

Signature: _____

Title: _____

Address: _____

Email Address: _____

Phone Number: _____

Fax Number: _____

Contact information to ask questions or learn additional information:

Name: _____

Title: _____

Address: _____

Email Address: _____

Phone Number: _____

Fax Number: _____