Sample Data Privacy Provisions for Vendor Agreements

1. COMPLIANCE WITH DATA PRIVACY STANDARDS FOR THE PROTECTION OF PII, PHI AND/OR PCI. Vendor acknowledges that to the extent it maintains, acquires, discloses, uses, or has access to any Organization Personally Identifiable Information ("PII"), as defined by state breach notification statutes, and/or any Organization Protected Health Information ("PHI"), as defined by the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, or Payment Card Information ("PCI)", as defined by the Payment Card Industry Data Security Standards ("PCI DSS"), Vendor shall maintain reasonable security procedures and practices appropriate to the nature of the PII, PHI and/or PCI, and protect the PII, PHI and/or PCI from unauthorized access, destruction, use, modification, or disclosure. Vendor is further obligated to comply with all relevant and applicable state, federal and international data privacy standards, including, but not limited to, California Civil Code §§ 1798.80-1798.84, Florida Information Protection Act, SB 1524, the Massachusetts Office of Consumer Affairs and Business Regulation Standards for the Protection of Personal Information, 201 CMR 17.00, Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), HIPAA and HITECH ("Data Privacy Standards"). Vendor represents and warrants that from the Effective Date of this Agreement and for so long as it maintains, acquires, discloses, uses, or has access to Organization PII, PHI and/or PCI thereafter, Vendor shall be in compliance with the Data Privacy Standards and that it shall notify the Organization in writing immediately if it is no longer in compliance with such Data Privacy Standards.

2. RETURN OR DESTRUCTION OF ORGANIZATION PII, PHI AND/OR PCI. If at any time during the term of this Agreement any part of Organization PII, PHI and/or PCI, in any form, that Vendor obtains from the Organization ceases to be required by Vendor for the performance of its obligations under this Agreement, or upon termination of this Agreement, whichever occurs first, Vendor shall, within fourteen (14) days, promptly notify the Organization and securely return such Organization PII, PHI and/or PCI to the Organization, or at the Organization's written request destroy, un-install and/or remove all copies of such Organization PII, PHI and/or PCI in Vendor's possession or control, or such part of the Organization's PII, PHI and/or PCI which relates to the part of the Agreement terminated, or the part no longer required, as appropriate, and certify to the Organization that the same has been completed.

3. USE OF SUBCONTRACTORS WITH ACCESS TO PII, PHI AND/OR PCI. When Vendor utilizes any third party, agent, other contractor, or subcontractor ("Subcontractor") in connection with or in furtherance of the services to be provided to the Organization under this Agreement and Vendor provides such Subcontractor with access to Organization PII, PHI and/or PCI, Vendor acknowledges and agrees that it shall first seek the approval of Organization for the use of such Subcontractor and will then provide Organization a summary of the extent of the role that such Subcontractor will play in connection with the performance of services provided to the Organization under the Agreement. Moreover, all such Subcontractors given access to any Organization PII, PHI and/or PCI must agree to: (i) abide by the terms

and conditions of this Agreement, including, without limitation, its provisions relating to compliance with Data Privacy Standards for the protection of PII, PHI and/or PCI and Notice of Security and/or Privacy Incident; (ii) restrict use of Organization PII, PHI and/or PCI only for Subcontractor's internal business purposes and only as necessary to render services to Vendor in connection with Vendor's delivery of services to the Organization, and (iii) certify in writing, upon completion of any services by a Subcontractor, that the Subcontractor has immediately un-installed, removed, and/or destroyed all copies of Organization PII, PHI and/or PCI within 14 days of such completion of services to Vendor.

4. NOTICE OF SECURITY AND/OR PRIVACY INCIDENT. If Vendor, or its Subcontractor, suspect, discover or are notified of a data security incident or potential breach of security and/or privacy relating to Organization PII, PHI and/or PCI, Vendor shall immediately, but in no event later than forty-eight (48) hours from suspicion, discovery or notification of the incident or potential breach, notify Organization of such incident or potential breach. Vendor shall, upon Organization's request, investigate such incident or potential breach, inform the Organization of the results of any such investigation, and assist the Organization in maintaining the confidentiality of such information. In addition to the foregoing, Vendor shall provide Organization with any assistance necessary to comply with any state and/or federal laws requiring the provision of notice of any privacy incident or security breach with respect to any Organization PII, PHI and/or PCI to the affected or impacted individuals and/or organizations, in addition to any notification to applicable state and federal agencies. Vendor agrees that it shall reimburse Organization for all expenses, costs, attorneys' fees, and resulting fines, penalties, and damages associated with such incident, breach, investigation and/or notification.

5. INSURANCE. Vendor agrees to purchase and maintain at all times, during the term of this Agreement, a professional liability insurance policy and a cyber liability insurance policy with coverage limits of at least $_____.

6. REMEDIES; DAMAGES; INDEMNIFICATION. Vendor shall bear all costs, losses and damages resulting from a breach of this Agreement. Vendor agrees to release, defend, indemnify, and hold harmless the Organization for claims, losses, penalties and damages and reasonable attorneys' fees and costs arising out of Vendor's, or its Subcontractor's, negligence, unauthorized use, disclosure, access, or acquisition (whether on their own or through a third-party) of Organization PII, PHI and/or PCI and/or Vendor's, or its Subcontractor's, breach of its obligations under this Agreement. Vendor acknowledges and agrees that it will inform all of its principals, officers, employees, agents and Subcontractors assigned to perform services for the Organization under the Agreement of the obligations contained herein. To the extent necessary and/or required by law, Vendor will provide training to such employees, agents and Subcontractors to promote compliance with this Agreement. Vendor agrees to assume all liability for breach of this Agreement by any of its principals, officers, employees, agents and Subcontractors.