Data Privacy Provisions for Vendor Agreements [for eRiskHub®]

Note: These provisions are provided as a template only. This is only a sampling of some of the data privacy provisions that should be included in vendor agreements. These provisions should be customized to fit the specific business, operational, and legal requirements of the Company.

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 Company Personally Identifiable Information ("PII"), as defined by state breach notification statutes, and/or any Company 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 Company PII, PHI and/or PCI thereafter, Vendor shall be in compliance with the Data Privacy Standards and that it shall notify the Company in writing immediately if it is no longer in compliance with such Data Privacy Standards.

2. RETURN OR DESTRUCTION OF COMPANY PII, PHI AND/OR PCI. If at any time during the term of this Agreement any part of Company PII, PHI and/or PCI, in any form, that Vendor obtains from the Company 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 Company and securely return such Company PII, PHI and/or PCI to the Company, or at the Company's written request destroy, un-install and/or remove all copies of such Company PII, PHI and/or PCI in Vendor's possession or control, or such part of the Company'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 Company that the same has been completed.

3. 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 Company 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 Company of such incident or potential breach. Vendor shall, upon Company's request, investigate such incident or potential breach, inform the Company of the results of any such investigation, and assist the Company in maintaining the confidentiality of such information. In addition to the foregoing, Vendor shall provide Company 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 Company 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 Company for all expenses, costs, attorneys' fees, and resulting fines, penalties, and damages associated with such incident, breach, investigation and/or notification.

4. 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 Company 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 Company 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 Company 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.