Information Security Exhibit

This Information Security Exhibit (this "**IS Exhibit**"), is attached to and incorporated into the Purchasing Agreement (the "**Agreement**"), by and between HealthTrust and Vendor. This IS Exhibit sets forth HealthTrust's required information security policies and procedures with respect to Vendor's provision of any Products and Services to all Purchasers. In the event of a conflict between the Agreement and this Exhibit, the Agreement shall control. Terms used in this IS Exhibit but not otherwise defined in this IS Exhibit will have the meaning set forth in the Agreement and any other applicable exhibits.

1. **APPLICATION AND TECHNOLOGICAL ADVANCES**. Vendor represents that Vendor's servers are currently located at a TierPoint data center to provide the SaaS Services, and no other provider. In the event Vendor intends to change such provider or add the use of a cloud service or other hosting provider, Vendor shall provide at least thirty (30) days prior written notice to HealthTrust. Upon such notification, HealthTrust, with Purchaser's approval, may terminate this Agreement for degradation of security obligations under this Agreement or other reasonable concern that remains outstanding after discussing in good faith with Vendor, and giving Vendor the opportunity to address, such concerns. HealthTrust and Vendor understand and agree that technologies and practices evolve over time, and that the administrative, physical, technical, and organizational measures and controls set forth in this IS Exhibit may be subject to progress and development. In that regard, Vendor and Subcontractors may, in some cases and upon the prior written approval of HealthTrust and Purchaser's approval (if applicable), implement alternative but equivalent (or functionally superior) measures to those set forth in this IS Exhibit; provided, however, that the implementation of such alternatives does not result in any degradation or reduction of the effectiveness of the associated measures and controls; and further provided, Purchaser's approval of the same shall not be deemed a waiver of any of Vendor's obligations under this IS Exhibit. In addition to, and without limiting Vendor's obligations under the Agreement, Purchaser may request, and Vendor shall not unreasonably refuse to enter into, a written undertaking to protect Purchaser's confidentiality and systems security in case of physical or on-line access to Purchaser's premises and/or Network.

2. **NETWORK ACCESS**. In addition to any requirements set forth in the Agreement, Vendor's access to Purchaser's Network is subject to the Purchaser's security and operational requirements as provided by Purchaser to Vendor. If granted access to Purchaser's Network, Vendor and Vendor Personnel shall only access those portions of the Network, application or data which they are expressly authorized by Purchaser to access, even if the technical controls in the Network, system or application do not prevent Vendor or Vendor Personnel from greater access. Notwithstanding the foregoing, Purchaser shall have in place reasonable and appropriate controls to prevent unauthorized access. Vendor shall impose reasonable sanctions against any Vendor Personnel who attempt to bypass security controls.

3. NETWORK ACCESS REMOVAL. Notwithstanding anything to the contrary in the Agreement or other agreement between Purchaser and Vendor, Purchaser in its sole discretion may refuse to grant Vendor or any Vendor Personnel access to Purchaser's Network or Confidential Information; Purchaser may at any time remove Network access from Vendor or any Vendor Personnel, without prior notice. In the event Purchaser withholds Vendor access other than in the event of Vendor's or Vendor Personnel's breach of this IS Exhibit, Purchaser shall be solely responsible for any outcome arising from Vendor's inability to access Purchaser's Network. Vendor shall make commercially reasonable efforts to replace Vendor Personnel within a reasonable period of time following any removal of access by Purchaser. Should Purchaser withhold Vendor access other than in the event of Vendor's or Vendor Personnel's breach of this IS Exhibit, Vendor shall not be responsible or liable for failure to perform the Services when no Vendor Personnel have access to Purchaser's Network.

4. VIRUS PROTECTION.

4.1 Equipment, Vendor Software and Local Software. With respect to any Products and/or Services which will be installed on and reside on Purchaser's Network, including, without limitation any Equipment, Vendor Software or Local Software installed on Purchaser's Network, Vendor warrants that such Products and/or Services, as applicable, will operate in conjunction with Anti-Virus Software, and will use real time protection features (provided, however, that the foregoing will be inapplicable to the successful operation of certain Vendor software directories and files, SQL server files and other similar exceptions that are outlined in, and pursuant to, Product Documentation).

4.2 Maintenance of Anti-Virus Software – On-Premise. The maintenance of the Anti-virus Software, including keeping current software updates and virus signature files, shall be the sole responsibility of the Purchaser for On-Premise Services. To ensure clarity, the Anti-Virus Software maintained by Purchaser for On-Premise Services must be updated at significantly frequent intervals necessary to maintain, at a minimum, current industry standard signature files and software updates.

4.3 Maintenance of Anti-Virus Software – SaaS Services. Vendor agrees that its maintenance of Anti-virus Software for SaaS Services includes keeping current software updates and virus signature files. To ensure clarity, the Anti-Virus Software maintained by Vendor for SaaS Services must be updated at significantly frequent intervals necessary to maintain, at a minimum, current industry standard signature files and software updates.

5. SECURITY STANDARDS.

5.1 Backups and Segregation

5.1.1 On-Premise. Purchaser shall be responsible for the management

and ongoing maintenance of its system backups and all Purchaser Data shall be logically segregated from other data in accordance with the Purchaser's applicable policies and procedures.

5.1.2 **SaaS Services.** Vendor shall be responsible for the management and ongoing maintenance of its system backups and all Purchaser Data shall be logically segregated from other customer data.

5.2 **Vulnerability Testing.** Vendor will engage an independent third party to conduct penetration testing on a yearly basis at Vendor's sole cost and expense. Such penetration testing shall include, without limitation, human manual testing, to evaluate the security controls of the application, host, and network layers used to provide any applicable Products and Services in accordance with industry standard methodologies (e.g., OWASP and OSSTMM). Such vulnerability testing will be completed within twelve (12) months of the Effective Date.

5.2.1 **Vulnerability Reports.** HealthTrust may, upon request, review at HealthTrust's site, with Vendor present, Vendor-controlled copies of such penetration testing reports (each, a "Vulnerability Report"). The Vulnerability Report should: (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Services, including without limitation Security Patches, upgrades, service packs, and updates to the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information reasonably needed for HealthTrust and Purchasers to evaluate the need for and the extent of their own precautionary or protective action. Vendor shall not hide or provide un-documented Security Patches in any type of change to its Product.

5.2.2 **Notification, Compensating Controls, and Corrective Actions**. Vendor will send notification to HealthTrust at security@healthtrustpg.com pursuant to Section 19.12 of the Agreement as soon as reasonably possible of any deficiencies identified as well as corrective or mitigating actions necessary for all vulnerabilities to be corrected or mitigated. Should any Critical Vulnerability be known to, or by exercising reasonable diligence should be known to, Vendor, Vendor shall notify Purchaser and provide Compensating Controls within seventy-two (72) hours of such discovery. If such Critical Vulnerability is publicly known, then Vendor shall, and will cause its Affiliates and Subcontractors (as applicable) to, make available to Purchaser Corrective Actions within thirty (30) calendar days of Vendor's discovery. If such Critical Vulnerability is known only to the Parties or their Affiliates

and Subcontractors (as applicable), Vendor shall make available to Purchaser Corrective Actions within sixty (60) calendar days of Vendor's discovery. For either type of discovered Critical Vulnerability, if Compensating Controls implemented by Vendor are mutually agreed by both Parties to be a mitigation with minimal impairment to Vendor Product functionality, then the Parties may mutually agree to a Corrective Action timeframe exceeding sixty (60) days. Should any weaknesses which are not Critical Vulnerabilities be identified, Vendor and its Affiliates and Subcontractors (as applicable) shall use reasonable efforts to provide Corrective Actions or Compensating Controls promptly, taking into account the CVSS(3) score of the weakness and the potential impact on Purchaser, in accordance with Vendor's standard internal procedure for correcting or mitigating vulnerabilities, but in no event later than sixty (60) days. Vendor shall use reasonable efforts to design any compensating controls in a manner that will minimize the impact of such controls on Purchaser. Notwithstanding the foregoing, to the extent a Critical Vulnerability exists with respect to hardware, software, and equipment (other than the Vendor's Software) installed at Purchaser's facilities, Purchaser shall be solely responsible for obtaining from the applicable third party, and implementing, compensating controls and corrective actions.

5.23 **SECURITY PATCH**. Unless otherwise expressly agreed by Purchaser and Vendor, Vendor's provision of the Products and Services includes, without limitation, Vendor's provision of Security Patches or compensating controls for the Products (subject to the lifecycle of the Products)[2], in each case, at no additional charge. Notwithstanding the foregoing, to the extent a Security Patch or compensating control is needed for hardware, software, and equipment (other than the Vendor's Software or equipment) installed at Purchaser's facilities, Purchaser shall be solely responsible for such cost.

5.3 **Encryption Procedures**. With respect to any Products and/or Services, including, without limitation, any Equipment, the Products shall support the encryption of all sensitive Purchaser Data in transit and at rest, subject to the support of compatible products and configuration selected by Purchaser. To the extent third-party products or Purchaser-selected configurations do not support encryption of sensitive Purchaser Data in transit, Vendor shall not be responsible. Vendor will, and as applicable and as possible, cause Affiliates of Vendor and Subcontractors to implement and utilize industry-accepted encryption products, methods, or algorithms to protect Purchaser Data and communications including, at a minimum, 256-bit VeriSign SSL

Certification and minimum 2048-bit RSA public keys, in the case of the Plum 360 pump and any newer models thereof; prior models of Product will meet the applicable standard set forth in their Documentation. All Personal Information at rest stored by the Software or SaaS Services, including any backups of such Personal Information, will be encrypted according to industry standard practices.

5.4 **Information Security Program.** Vendor will develop, maintain, and implement a comprehensive written information security program that complies with applicable privacy laws, and includes, without limitation, mandatory training to Vendor Personnel regarding the privacy, confidentiality and information security requirements set forth in the Agreement and this IS Exhibit with regard to Personal Information. Vendor's information security program will include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to: (a) protect the security and confidentiality of Personal Information; (b) protect against any anticipated threats or hazards to the security and integrity of Personal Information including implementing appropriate risk management practices according to the NIST framework (including, without limitation, those NIST standards applicable to pumps); (c) protect against any Information Security Incident; and (d) protect against the use of the Products and Services and Purchaser Network or Vendor Network as a portal to give unauthorized access to any other systems of Purchaser or its Affiliates. Vendor will, upon prior written request, share with HealthTrust its information security program information during an on-site visit to Vendor, but no more than once annually. Nothing herein shall prevent HealthTrust from requesting the information required under this Section in the event of an Information Security Incident.

6. INFORMATION SECURITY INCIDENT.

6.1 Notification and Response. In addition to the notification requirements in any Business Associate Agreement with or for the benefit of Purchaser, in the event Vendor discovers any Information Security Incident, Vendor shall, at its sole expense: (a) expeditiously (but in no case later than twenty four (24) hours after such discovery) report such Information Security Incident to HealthTrust and each affected Purchaser, summarizing the Security Incident in reasonable detail including, at minimum, to the extent known to Vendor: (i) the date and time when the Information Security Incident occurred; (ii) the date and time when such incident was discovered by Vendor; (iii) identification of the systems, programs, Vendor Network, Purchaser Network and/or Purchaser Data affected by such incident ("Initial Notification"); (b) provide a preliminary impact analysis; (c) investigate such Information Security Incident, perform a risk assessment, and develop a corrective action plan; (d) prepare and implement a remediation plan to take all reasonably necessary and advisable corrective actions and cooperate

with any affected Purchasers in all reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident; (e) make key Vendor Personnel involved in the remediation plan reasonably available to respond promptly to HealthTrust and each affected Purchaser; and (f) cooperate with HealthTrust and each affected Purchaser in providing any filings, communications, notices, press releases or reports related to any Information Security Incident ("Subsequent Notification"). For the avoidance of doubt, it is not required for HealthTrust to approve the Initial Notification.

6.2 **Security Incident Contact Person.** Vendor shall promptly designate a contact person for HealthTrust and each Purchaser to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (a) act as a liaison to communicate between Vendor and HealthTrust and between Vendor and Purchaser regarding the Information Security Incident (including providing information requested by HealthTrust and/or Purchaser); (b) perform the reporting obligations of Vendor; and (c) develop a mitigation strategy to remedy or mitigate any damage to Purchaser Network, Purchaser infrastructure, Purchaser Data, Products, Services or Vendor Network(s) that may result from the Information Security Incident.

6.3 **Indemnification.** In addition to the indemnification obligations of Vendor set forth in the Agreement and any business associate agreement, but subject to Section 10.2 of the Agreement, Vendor will defend, indemnify and hold Purchaser, its Affiliates, and their respective officers, directors, employees and agents, harmless from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorney fees, arising out of or relating to any third party claim arising from any Information Security Incident to the extent such Information Security Incident results from a breach of Vendor's obligations under this IS Exhibit relating to privacy or security, including but not limited to: (a) expenses incurred to provide warning or notice to Purchaser's former and current employees, suppliers, customers, patients and other persons and entities whose Personal Information may have been disclosed or compromised as a result of the Information Security Incident (the "Affected Persons") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, or as otherwise directed by Purchaser; (b) expenses incurred either by Purchaser or through Purchaser's retention of an independent third party forensic investigator, legal counsel, or any other third party, to investigate assess or remediate the Information Security Incident and to comply with applicable law and/or relevant industry standards; (c) expenses related to the reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to costs associated with the offering of credit monitoring for a period of at least twelve (12) months or such longer time as is required by law or recommended by one or more of Purchaser's

regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (d) fines, penalties, or interest that Purchaser pays to any governmental or regulatory authority; (e) legal expenses incurred in connection with a Information Security Incident or to address any claims by third parties as a result of the Information Security Incident or investigation by law-enforcement agencies or regulatory bodies; and (f) expenses incurred to the retention of a public relations or crisis management firm in order to manage communications on behalf of Purchaser related to any Information Security Incident. Notwithstanding the foregoing, Vendor shall not be liable in any event for lost profits, consequential, indirect, punitive, exemplary or special damages, nor shall Vendor be liable for any costs or expenses or other amounts related to or due as a result of any government investigation or enforcement action to the extent arising from Purchaser's own misconduct, breach of or noncompliance with its contractual, regulatory or legal obligations.

6.4 **Termination.** The occurrence of an Information Security Incident, to the extent such Information Security Incident results from a breach of Vendor's obligations under this IS Exhibit relating to privacy or security and to the extent such Information Security Incident results in material harm to Purchaser, is grounds for Purchaser to terminate any unfulfilled orders for Products and Services from Vendor, applicable Purchaser Agreements (if any) and applicable Ordering Documents (if any) for cause.

7. VENDOR PERSONNEL.

7.1 **Vendor Personnel.** Vendor agrees to disclose to Purchaser the names of Vendor Personnel who will access Purchaser's Network(s). Such designation shall include the full name of the Vendor Personnel and a mutually agreed identification number for each Vendor Personnel. Each of Vendor Personnel having access to any part of a Purchaser's Network shall: (a) be assigned a separate log-in ID by the Purchaser and uses only that ID when logging on to the Purchaser's Network; (b) log off the Purchaser's Network immediately upon completion of each session; (c) not allow other individuals to access the Purchaser's Network; and (d) keep strictly confidential the log-in ID and all other information that enables access.

7.2 **Vendor Personnel Confidentiality.** Any Vendor Personnel including agents, independent contractors, or subcontractors of Vendor that will access the Purchaser Network shall be required to have entered into a written agreement containing terms consistent with, and at least as restrictive as the confidentiality and data security terms of the Agreement before receiving access to the Purchaser Network.

7.3 **Termination of Vendor Personnel; Purchaser Revisions to Access Requirements.** Vendor must promptly notify each Purchaser upon termination of employment or reassignment of any of Vendor Personnel with access to Purchaser Network. If any Purchaser revises the requirements

for access to its Network, then the Purchaser must notify Vendor of the changed or additional requirements and Vendor must comply with them as a prerequisite to continued access. Any Purchaser may require each individual who is to be allowed access to that Purchaser's Network to acknowledge the individual's responsibilities in connection with the access.

8. SERVICE.

8.1 Account Usage. Upon request, Vendor shall provide Purchaser with a list of active Vendor Personnel with access to Purchaser Network(s) user accounts for Purchaser to deactivate or disable access to Purchaser's Network if Purchaser deems appropriate.

8.2 Purchaser Network Access Requirements.

8.2.1 If Purchaser provides Remote Access to any Purchaser Network for maintenance or support services, Vendor shall comply with the Purchaser's Remote Access security requirements in addition to any other security requirements set forth in the Agreement. Before Vendor may remotely access any Purchaser's Network, the Purchaser may require prior certification that Vendor complies with the Purchaser's security policies and standards.

8.2.2 Vendor shall only use Products, Services and Vendor Network(s) which are compatible with Vendor-approved Purchaser Remote Access technology in order to access Purchaser Network. If Vendor does not have Products, Services and Vendor Network(s) that are compatible, it is Purchaser's responsibility to obtain Products, Services and Vendor Network(s) which are compatible with Purchaser's Network, at Purchaser's cost.

8.2.3 Vendor shall implement reasonable security controls on Vendor's systems or equipment under Vendor's control to protect Purchaser's Network from risk when its systems or Vendor Personnel connect to the Purchaser Network. Such controls include, but are not limited to installing and maintaining ICSA Labs certified Anti-virus Software on Products, Services and/or Vendor Network(s) and, to the extent possible, the use of real time protection features. Vendor shall maintain the Anti-virus Software in accordance with the Anti- virus Software vendor's recommended best practices.

8.2.4 Vendor may not access the Purchaser Network with any Products, Services or Vendor Network(s) that may allow bridging of the Purchaser Network to a non-Purchaser Network without approval from the Purchaser.

9. RISK MANAGEMENT REQUIREMENTS.

9.1 Security Controls. The Products, Services and Vendor Network(s) will provide, where applicable, configurable security controls including, at a minimum: (a) the ability to revoke access to the Products, Services and Vendor Network(s) after a defined number of consecutive failed login attempts ("Lockout"); (b) the ability to specify the Lockout time period; (c) the ability to specify the number of invalid login requests before initiating the Lockout; (d) controls to provide that system-generated initial or reset passwords must be changed by the End User upon first successful use; (e) controls to terminate an End User session after a defined period of inactivity; (f) password history controls to limit password reuse; (g) password length controls; (h) password complexity requirements; (i) the ability to accept logins to the Products, Services and Vendor Network(s) only from certain IP address ranges upon configuration at the Purchaser firewall on its VLAN); and (j) the ability to delegate End User authentication or federate authentication via LDAP. The Products, Services, and/or Vendor Network(s) will not provide the foregoing where such configurable security controls are dependent on using LDAP integration with the Purchaser's network.

9.2 End User Credentials.

9.2.1 Vendor Responsibilities – SaaS Services. For the provision of SaaS Services, each End User shall be assigned a unique user ID and password, token, or biometric identifier ("Credentials"), and Vendor will allow End Users to access the Products, Services and Vendor Network(s) only after authentication with valid Credentials. Credentials will be stored at rest using a one-way hashing algorithm (SHA-256, or the equivalent), and will be encrypted whenever transmitted over the Internet or any untrusted network, using Secure Sockets Layer ("SSL") protocol during transmission. Upon authentication, the Vendor Software will provide the ability to track each End User's activity through the use of a unique session identifier associated with the user ID and each login session. In any instance in which a password is created other than through direct selection by the End User, such password will be valid only for one successful login, upon which the receiving End User will be required to manually select a replacement password. Vendor Software shall have the ability to use identity and access management standards such as identity and access management standards such as LDAPS, OAuth, OpenID Connect in order to make authentication and authorization decisions. In no instance will Vendor Personnel manually select and assign a password to an End User, except for the initial password for the MedNet Product.

9.2.2 Purchaser Responsibilities. Purchaser shall cause each End User to: be one of those persons or classes of persons, as appropriate, in its workforce or subcontractors who need access to the Products or Services to carry out their duties; use the Products and Services only in accordance with applicable law and Purchaser's policies and procedures; agree to keep his or her Credentials confidential and not share them with any other person except as permitted or required by law; agree to notify Purchaser and Vendor promptly after discovery, any Breach or Security Incident, including the theft or loss of an End User's Credentials.

9.3 Retention and Destruction of Purchaser Data. During the term of the Agreement and as otherwise obligated under the Agreement, Vendor will not delete or destroy any Purchaser Data or media on which Purchaser Data resides without prior authorization from Purchaser. Purchaser hereby authorizes Vendor to delete or destroy Purchaser Data in accordance with any Purchaser document retention policies furnished to Vendor in writing. In the event any Purchaser Data is lost or destroyed due to any act or omission of Vendor, including any Information Security Incident, Vendor shall restore such Purchaser Data using the most recent available back-up. Vendor shall prioritize this effort to minimize any adverse effect upon Purchaser's business or use of the Products or Services. Purchaser agrees to cooperate with Vendor to provide any available information, files, or raw data needed for the regeneration, reconstruction, or replacement of the Purchaser Data. If Vendor fails to fully regenerate, reconstruct and/or replace any lost or destroyed Purchaser Data within the time reasonably set by Purchaser, then Purchaser may, at Vendor' expense, obtain data reconstruction services from a third party, and Vendor shall cooperate with such third party as requested by Purchaser. If it is determined that Purchaser Data has been lost or destroyed as a result of the willful, intentional, or grossly negligent acts or omissions of Vendor, Purchaser may terminate this Agreement for cause and pursue any civil and criminal actions available to it.

10. INFORMATION SECURITY AUDIT. In addition to any audit rights provided to HealthTrust under the Audit Rights Section of the Agreement, Purchaser, HealthTrust or an external auditing firm selected by HealthTrust which is not a competitor of Vendor shall have the right to audit Vendor's compliance with this IS Exhibit as provided in this Section 10.

10.1 Logging. The Products, Services and Vendor Network(s) will provide, where applicable, the following minimum logging capabilities: (a) firewalls, routers, network switches and operating systems, will have their respective logging capabilities enabled, active, and configured to record, to their respective default logging destination or to a centralized syslog server (for network systems), event records in sufficient detail for diagnostic and analytical purposes in the event of an actual or suspected unauthorized

access to or misuse of the Products, Services and Vendor Network(s); (b) records of End User access log entries containing, at a minimum, the date, time, user ID, success of operation; (c) all required log records will be maintained for a minimum of ninety (90) days; (d) all required log records will be kept physically and virtually secured to prevent tampering; (e) passwords will not be logged under any circumstances; and (f) certain administrative changes to the Products, Services and Vendor Network(s) (such as password changes, privilege modification and account creation or deletion) will be tracked in an "Setup Audit Log" available, upon request, for viewing by Purchaser's system administrators. Vendor will, upon reasonable prior written request, provide to HealthTrust and/or external auditing firm selected by HealthTrust or an entity designated by HealthTrust, copies of any log files reasonably requested to assist in the analysis or investigation of any actual or suspected unauthorized access or misuse of any Products, Services and Vendor Network(s) affecting Purchasers, Purchaser's Network or any Affiliate of Purchasers.

10.2 **Internal Review and Audit Report**. If Vendor is providing SaaS Services, upon request by HealthTrust and/or an external auditing firm selected by HealthTrust, Vendor shall provide a copy of Vendor's then-current report on controls within Vendor's organization and systems under Statement on Standards for Attestation Engagements (SSAE) No. 16 (or No. 18, as applicable), or under standards established by an authorized or recognized standard setting organization (such as the International Auditing and Assurance Standards Board). Such review and report will be conducted at Vendor's operations center at Vendor's cost for reasonable travel expenses only by an independent auditing firm for the purposes of verifying the safety and soundness of the Products and/or Services. As of the Effective Date, Vendor is not in possession of any SSAE report. If, upon request by HealthTrust and/or an external auditing firm selected by HealthTrust, Vendor is not in possession of an SSAE report, then Vendor shall have until the end of its third fiscal quarter following such request to acquire such report or an equivalent report. Nothing herein shall require Vendor to pay the professional fees or other costs of HealthTrust's engagement of an external auditing firm.

10.3 **Certificates.** Vendor's Managed Service Provider has in the past obtained HITRUST certification. Vendor shall update such HITRUST certification within the first six (6) months after the Effective Date. If Vendor is providing SaaS Services, Vendor shall obtain by the end of its third fiscal quarter following the issuance of a future iteration of Vendor Product, and shall update annually: (a) a Service Organization Control 2 ("SOC 2") Type II report (or any successor reports) for security availability, confidentiality, and privacy-related controls of the information processing and management systems (including procedures, people, software, data, and infrastructure) used by Vendor and its subcontractors in storing, accessing, and processing of Purchaser Data received by Vendor under the Agreement, and (b) a ISO

27001/27002 certification or industry-standard successor report. Vendor may continue to obtain HITRUST certification for such Product iteration in lieu of both a SOC 2 Type II or successor report and ISO 27001/27002 certification or industry-standard successor report. Vendor will promptly provide a copy of the SOC 2 report and ISO certification report, or HITRUST certification, to HealthTrust and/or an external auditing firm selected by HealthTrust , and in no event later than thirty (30) days of receipt from the independent auditor or certification body for each annual period in which Vendor receives the same. Vendor will promptly notify HealthTrust and/or an external auditing firm selected by HealthTrust of any deficiencies identified in any reports. Vendor will promptly address and resolve any such deficiencies to the extent necessary to comply with Vendor' obligations under this Agreement, and also notify HealthTrust and/or an external auditing firm selected by HealthTrust when any such deficiency is resolved. If any deficiency is not promptly resolved, it shall be deemed a material breach of this Agreement by Vendor.

10.4 **Compliance Audit**. HealthTrust shall have the right, at its expense, during normal business hours and with reasonable advance notice, to evaluate, test, and review at Vendor's premises, Products, Services and Vendor Network(s) to ensure compliance with the terms and conditions of the Agreement and this IS Exhibit. HealthTrust shall have the right to conduct such audit by use of its own employees and internal audit staff, or by use of an external auditing firm selected by HealthTrust. Vendor shall cooperate with and provide reasonable assistance to HealthTrust and provide all pertinent books and records (including, but not limited to, system and facility maintenance records, Product and Service Vulnerability Reports, relevant Audit Log files and Vendor's internal information security assessment report) and other information reasonably requested by HealthTrust in connection with such audit at no additional cost to HealthTrust. Notwithstanding the foregoing, such evaluation, testing, or review by HealthTrust under this Section shall not be conducted for more than one week's time, and no more frequently than bi-annually. HealthTrust audits as permitted by Section 5.1 shall not be subject to the foregoing limitation.

11. **CYBER RISK AND DATA SECURITY INSURANCE.** Vendor will maintain at its own expense, with such other terms and conditions as reasonably required by Purchaser and/or any applicable Affiliate(s) cyber risk and data security insurance with limits not less than five million dollars ($5,000,000.00) per occurrence.

12. **DEFINITIONS**.

12.1 "**Anti-virus Software**" shall be defined as industry-standard software specifically written to prevent the introduction or intrusion of Malicious Software.

12.2 "**Audit Log**" means a time-based record of system activities to enable the audit, reconstruction, and examination of the sequence of events and/or changes in an

event, including without limitation, who accessed a system and what operations the person has performed during a given period of time.

12.3 **"Compensating Control"** means a mechanism that is put in place to satisfy the requirement for a security measure that is deemed by Vendor to be too difficult or impractical to implement at the present time.

12.4 **"Corrective Action"** means an action to eliminate the cause of a detected non-conformity or undesirable situation, as defined by the U.S. Food and Drug Administration.

12.5 "**Critical Vulnerability"** means any Vulnerability with a Common Vulnerability Scoring System Revision 3 ("**CVSS(3)**") score of 7 or above.

12.6 **"Vulnerability**" means a flaw or weakness in a Product's or system's security procedures, internal controls, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in harm or unauthorized access to a system, activity or Purchaser Data.

12.7 "**End User**" means an individual that Purchaser permits to use the SaaS Services, which may include, without limitation, employees agents, contractors, consultants, outsourcers, suppliers or other individuals (including third parties), but only in accordance with Section 9.2.2.

12.8 "**Information Security Incident**" means: (a) the actual unauthorized acquisition, access, use, processing, loss or disclosure of Purchaser Data; (b) the suspicion or reasonable belief that there has been an unauthorized acquisition, access, use, processing, loss, disclosure of Purchaser Data or (c) the unauthorized use of any Products or Services to gain access to any Purchaser Network or Vendor Network or (d) any other event which results in or in Vendor's reasonable judgment may result in harm or damage to a system or data or unauthorized access or disclosure of data or information.

12.9 "**Local Software**" means any software provided by Vendor for local installation and use in connection with the SaaS Services.

12.10 "**Malicious Software**" shall be defined as any type of software or program which is designed to: (a) cause unauthorized access to or intrusion upon; or (b) otherwise disrupt and/or damage, computer equipment, software, and/or data (commonly referred to as a virus, worm, Trojan horse, or spyware)

12.11 "**Network**" means a configuration of computers, workstations, and other devices that are inter-connected.

12.12 "**Ordering Documents**" means the ordering documents entered into by and between the Purchaser and Vendor for the purchase and order of Products and Services, and includes, without limitation, any Statements of Work, as applicable.

12.13 "**Personal Information**" means any information relating to an identified or identifiable individual (such as name, postal address, email address, telephone number, date of birth, Social Security number (or its equivalent), driver's license number, account number, personal identification number, health or medical information, or any other unique identifier or one or more factors specific to the individual's physical, physiological, mental, economic or social identity), whether such data is in individual or aggregate form and regardless of the media in which it is contained, that may be (a) disclosed or processed at any time to Vendor by Purchaser or an Affiliate; or (b) derived by Vendor from the information described in (a).

12.14 "**Purchaser Data**" means any or all Personal Information that is stored, recorded, processed, created, derived or generated by Vendor for or on behalf of the Purchaser, regardless of the form or media in which such data is held.

12.15 "**Remote Access**" means the connectivity which enables access from a network outside the Purchaser Network to the perimeter of the Purchaser Network.

12.16 "**Security Patch**" means a patch, bug fix, software update, upgrade, modification, improvement, enhancement, or fix (i) designed to repair known problems in previous software releases in order to prevent unauthorized access, destruction, or corruption of data, or exploitation of Vulnerability and (ii) that occurs between regularly-scheduled new releases or new versions.

12.17 "**SaaS Services**" means the software-as-a-service ("SaaS") services and all software used by Vendor to display and perform the SaaS Services.

12.18 "**Software**" means any and all computer software licensed to Purchaser under applicable Exhibits. The term Software includes, as applicable and without limitation, software provided through or in relation with the SaaS Services, Local Software (as defined in the Software as a Service Terms and Conditions Exhibit, if applicable) and Vendor Software (as defined in the On Premise Software Terms and Conditions Exhibit, if applicable).