Compliance and Information Security Terms

Unless otherwise defined herein, capitalized terms shall have the same meaning as set forth in the Agreement.

1. **Equal Employment Opportunity ("EEOC")**

   If the combined fees to be paid by CLIENT for Services under the Agreement is more than $10,000.00, then VENDOR and its Personnel (including subcontractors) shall abide by the requirements of 41 CFR 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities and prohibit discrimination against all individuals based on their race, color, religion, sex, or national origin. Moreover, VENDOR and its subcontractors shall take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability.

2. **Code of Conduct/ Corporate Compliance Program**

   If VENDOR's Services will be provided at CLIENT's locations or facilities, or if VENDOR or VENDOR's Personnel are acting on behalf of CLIENT, then VENDOR certifies that their Personnel are expected to perform their work for CLIENT in a manner consistent with the principles set for in CLIENT's Code of Conduct ("**Code**") located at https://www.jointcommission.org/code_of_conduct/.

3. **Background Verification**

   If VENDOR is providing Services or products which may be paid for by federal healthcare program dollars, then VENDOR represents and warrants to CLIENT that all VENDOR Personnel provided to CLIENT under the Agreement:

   A. Are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any federal agency;

   B. Have not been found guilty of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; or

   C. Have not been found guilty of commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property.

   VENDOR agrees to promptly inform CLIENT of the imposition of any such sanctions or exclusion and of the initiation of any investigation or proceeding the result of which may include such sanctions or exclusion regarding any VENDOR Personnel involved in the provision of Services. The Agreement may be subject to immediate termination in the event VENDOR or its Personnel are subject to sanctions or exclusion. And upon request, VENDOR shall provide documentation to CLIENT of the above designated appropriate background clearance for all Personnel providing the Services.

4. **Data & Privacy**

   A. Business Associate Agreement

If VENDOR or VENDOR Personnel will have access to or use of any protected health information ("**PHI**"), as this term is defined by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), VENDOR hereby agrees to be bound by CLIENT'S Business Associate Subcontractor Agreement ("**BAA**") located at https://www.jointcommission.org/terms-of-use/legal-documents/

.

B. Data Processing Agreement

C. If VENDOR or VENDOR Personnel will have access to or use of any data or information that identifies or can be used to directly or indirectly identify, contact, locate, or is otherwise related to an individual ("**Personal Data**") under applicable data privacy, data protection, and data security laws and regulations ("**Applicable Privacy Laws**"), then, VENDOR hereby agrees to be bound by the terms of The Joint Commission Enterprise Vendor Data Protection Exhibit ("**Data Protection Exhibit**") located at https://www.jointcommission.org/terms-of-use/legal-documents/

D. PCI Compliance

If VENDOR processes credit card transactions, then it represents and warrants that it meets PCI compliance standards.

E. Identity Theft Plan

If VENDOR will have access to or use of personally identifiable information, as this term is defined by NIST SP 800-53 Rev. 4 under Personally Identifiable Information (OMB Memorandum 07-16), then VENDOR represents and warrants that it will maintain an identity theft plan and program.

5. **Information Security Requirements**

If VENDOR or VENDOR Personnel will have access to CLIENT's systems, data, or information, then VENDOR agrees to the following:

A. General

VENDOR shall maintain industry standard internet, application, information system security throughout the provision of Services to CLIENT. Such controls shall include antivirus, firewalls, and security tools which meet or exceed government minimum requirements for security. In addition, VENDOR warrants that:

1. User identification and access controls are designed to limit access to Confidential Information to VENDOR Personnel who have received permission from CLIENT to access Confidential Information. VENDOR shall conduct an annual review to ensure compliance with this provision;

2. Encryption will be used for all CLIENT data at rest and in transmission and shall comply with current NIST, or agreed upon, encryption standards;

3. All patches are installed promptly and remain up to date and that third-party software that is no longer supported will not be used for the Services;

4. Confidential Information will be stored on a secure server, in locked data cabinets within a secure facility which is located within the jurisdiction of the United States. Only authorized VENDOR Personnel will have physical access to such information;

5. External connections to the internet will have appropriate security controls including industry standard intrusion detection and countermeasures that will detected and terminate any unauthorized activity prior to entering the firewall maintained by VENDOR;

6. Firewalls shall regulate all data entering the VENDOR software from any external source, will enforce secure connections between internal and external systems, and will permit only specific types of data to pass through;

7. It will maintain and follow a disaster recovery plan designed to maintain CLIENT's access to the Services, and to prevent the unintended destruction of CLIENT data or Confidential Information. In no event shall the Services, Confidential Information and/or CLIENT data be unavailable to CLIENT for a period in excess of twenty-four (24) hours;

8. Its information security plan conforms to a recognized cybersecurity framework designed for that purpose.[1]

B. Reporting

VENDOR and VENDOR's Personnel will immediately report any actual or attempted security violations or potential breach of Confidential Information to CLIENT's Chief Information and Security Officer.

C. Admin, Phys, Tech Safeguards

VENDOR shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any CLIENT information as are necessary to prevent the use or disclosure of such information other than as permitted by the Agreement.

D. Access/Use

VENDOR will ensure Personnel will only access and use computer equipment/systems as authorized, to maintain login and passwords in a confidential manner and not further disclose, to not disclose any portion of computerized system or information to unauthorized individuals. This includes but is not limited to design, programming techniques, flow charts, source code, screens and documentation created by VENDOR under the agreement or created by any CLIENT personnel to which VENDOR has been provided access.

VENDOR shall ensure that Confidential Information will only be disclosed to authorized third parties who have agreed to the same levels of protections that apply to VENDOR.

[1] Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, IS0 27002, NIST SP 800-53 and NIST SP 800-171.

VENDOR shall immediately report to CLIENT in the event of an occurrence of unauthorized access, use or disclosure of CLIENT Confidential Information.

E. Data Segregation

VENDOR agrees to maintain controls which logically segregate CLIENT applications, systems, Confidential Information and share such applications and data only with third parties when specifically authorized by CLIENT in accordance with the agreement.

F. Testing

VENDOR shall conduct regular testing of the systems and procedures outlined in this section and provide for an annual risk assessment to maintain industry standard security safeguards. VENDOR commits to addressing all findings noted on the annual risk assessment in a timely manner as dictated by the severity. Audit controls shall record and monitor Services activity continuously. VENDOR shall provide a copy of any of the following: a Hitrust CSF certification, or a third-party risk assessment for HIPAA and NIST 800-53, ISO 27001, or a third party SSAE18, Type II, and SOC2 Type II report. To the extent the above documents do not contain a management response section, VENDOR will provide a list of findings, action taken or to be taken and timing of expected resolution. Results are to be made available to CLIENT as soon as they are completed. Upon request, VENDOR will provide crosswalk of audited standards to NIST 800-171 and GDPR standards.

G. Audit Rights. CLIENT retains the right to review the third party audit of VENDOR's information systems security program on a periodic basis or participate in an audit when a security concern arises. Failure to conduct the audit in no way waives the right to do so.

H. Security Questionnaire

VENDOR agrees to answer an annual security questionnaire if requested and provided by CLIENT.

I. Notification of Material Security, System, or Infrastructure Changes and Vulnerability Disclosures

VENDOR must notify CLIENT of material changes in VENDOR's security posture, systems or IT infrastructure, within twenty (20) business days of such change. And VENDOR must update its information security plan no later than fifteen (15) days into the next calendar quarter and must provide updated evidence of compliance with the information security plan.

J. Data Deletion

At CLIENT'S request, or upon termination of this Agreement, VENDOR shall delete and return CLIENT'S data and information, including customer data/information and Personal Information ("Personal Information" means all information that identifies or can be used to directly or indirectly identify, contact, locate, or is otherwise related to an individual), except where VENDOR is required to retain copies under applicable laws, in which case VENDOR must communicate in writing to CLIENT the legal basis preventing it from returning or destroying CLIENT'S data and information, and warrants that is shall guarantee the protection, security, and confidentiality of any such data for so long as VENDOR retains it. Further, CLIENT hereby instructs VENDOR, and VENDOR agrees, to delete any and all Personal Information within a reasonable time period in line with data protection laws once the Personal Information is no

longer required for VENDOR to fulfill the services under this Agreement, except where VENDOR is required to retain copies under applicable laws, in which case VENDOR must communicate in writing to CLIENT the legal basis preventing it from returning or destroying the Personal Information, and warrants that is shall guarantee the protection, security, and confidentiality of any such data for so long as VENDOR retains it. Upon request, VENDOR shall provide CLIENT with an Officer's Certificate or other proof acceptable to CLIENT to certify its compliance with this provision.

6. **Subcontractor Requirements**

If VENDOR uses subcontractors for the performance of any of the Services under the Agreement, then VENDOR shall maintain, and provide upon request, a list of all subcontractors being used for the performance of any of the Services to be performed under the Agreement. VENDOR shall ensure that all such subcontractors are bound in writing to the same terms in this Compliance and Information Security Terms that are applicable to VENDOR.

7. **Conflicts of Interest/Related Party transactions**

If VENDOR or VENDOR's Services constitute a conflict of interest with CLIENT, then VENDOR shall identify in writing any personal, financial, referral or other business relationship(s) with any CLIENT board member, officer or employee. Unless CLIENT has provided prior written consent, VENDOR shall confirm that there exists no actual or potential conflict between VENDOR's family, business or financial interest and its Services under the Agreement.

8. **International Business Practices**

If VENDOR Services involve work with foreign government officials on behalf of CLIENT, then VENDOR, along with its Personnel, agrees to comply at all times with CLIENT's International Business Practices Policy, which shall be provided upon VENDOR's request, and to sign a policy compliance attestation upon request.

9. **Update to Terms**

CLIENT reserves the right to modify the terms contained herein, including the terms associated with any linked documents or policies, at any time without prior notice to VENDOR.