Information Security Program

1) **Definitions**

a. Capitalized terms, not otherwise defined herein shall have the same meaning as defined in the Master Agreement shall have the meanings ascribed to them under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the HITECH Act and the related regulations promulgated by HHS (collectively, "HIPAA") or the Master Agreement between the Parties, as applicable.

b. "Backdoors" shall mean a method of bypassing normal authentication or securing remote access to a computer.

c. "Successful Security Incidents," for purposes of this Information Security Program, shall mean a security incident that results in the unauthorized access, use, disclosure, modification, or destruction of Client Data, including PHI. For the avoidance of doubt, Successful Security Incident shall NOT mean a security incident that does not result in unauthorized access, use, disclosure, modification, or destruction of Client Data or PHI (including, for example, and not for limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses).

2) Company General Requirements and Definitions

a. Security Program. Company shall maintain a comprehensive security program under which Company documents, implements and maintains the physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of Company systems and infrastructure and Client Data and comply with applicable privacy and security Laws and the requirements of this ISP.

b. Company Security Contact. Company shall designate one or more privacy and data security contacts who are responsible for overseeing compliance with this ISP and provide Client with contact information for these security representatives, upon request.

c. Policies and Procedures. Company shall maintain written security management policies and procedures designed to identify, prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, availability, or security of Company systems and infrastructure and Client Data. Such policies and procedures shall: (a) assign specific data security responsibilities and accountabilities to relevant teams; (b) include a formal risk management program which includes periodic risk assessments at least annually to ensure continued compliance with obligations imposed by Law or contract; and (c) provide an adequate framework of controls that safeguard Company systems and infrastructure, Client systems which Company has access to, and Client Data.

d. Subcontractors. To the extent that any current Company subcontractor accesses Client Data or creates, has access to, or receives from or on behalf of Client any Client Data in electronic format, Company represents that such subcontractors are subject to a reasonable written agreement governing the use and security of Client Data. Prior to providing any new Company subcontractor with access to Client Data, or prior to new Company subcontractor creating or receiving any Client Data in electronic format, Company shall obtain reasonable written agreement governing the use and security of Client Data.

3) Security Risk Assessment

a. Assessment. Company shall conduct a security risk assessment no less than annually for assurance of controls that address current legal, regulatory and security requirements ("Security Assessment"). As part of Company's compliance program for certification/accreditation, evidence of HITRUST CSF or SOC 3, or the then current alternate industry standard security certification, will validate that a security risk assessment has been conducted.

b. Remediation Requirements. If the Security Assessment reveals that Company does not meet any of the requirements of this ISP or the Master Agreement, then Company shall complete such remediation requirements, within a reasonable timeframe.

4) Independent Certification

a. Independent Certification Requirements. Company will maintain an Independent Certification, as further set forth in this Section 4, until the later of: (a) the expiration or earlier termination of the Master Agreement; or (b) Company no longer maintains (including in archived or secure storage) or otherwise has access to, any Client Data. As used herein, "Independent Certification" means the approved certification(s) or attestation(s) listed below, in each case covering all Company systems and infrastructure and Company providing Services contracted for in the Master Agreement, as well as applicable Company facilities used in connection with the provision of the Services.

b. Acceptable Independent Certifications or Attestations.

Certification/Attestation	Conditions
HITRUST r2 Certification	Company shall maintain a two-year HITRUST r2 certification covering all Company systems and infrastructure
SOC2 Type II	Company shall maintain SOC 2 Type II annually

c. Supplementary Documentation. Upon Client request, and no more than annually, Company will provide supplementary documentation as described below to Client to verify that the scope of certification or attestation covers the scope of Services.

Certification/Attestation
Letter of HITRUST r2 Certification
SOC 3

5) Security Incident Response

a. General. Company shall maintain formal processes to detect, identify, report, respond to, contain, and resolve Successful Security Incidents in a timely manner.

b. Report. Report to Client any Successful Security Incident, within thirty (30) business days. When applicable, as soon as reasonably possible, Company shall supplement with a written report containing any information known to the Company at that time.

c. Security Incidents – Containment. Company will promptly commence containment processes during any incident investigation.

6) Baseline Security Requirements

a. Infrastructure Protection. Company shall maintain commercially reasonable industry standard controls to protect Company systems and infrastructure, including, at a minimum:

i. Data loss prevention mechanisms designed to segment, monitor, restrict, and prevent Client Data from moving to unauthorized internal or external network locations.
ii. Router filters, firewalls, intrusion detection and prevention systems, and other network mechanisms to restrict access to the Company systems and infrastructure, including without limitation, all local site networks that may be accessed via the Internet (whether or not such sites transmit information);
iii. Resources used for mobile access to Client systems, if any, shall be protected against attack and penetration through the use of firewalls, malware detection/prevention, and encryption;
iv. Processes to prevent, detect, and eradicate malicious code; and
v. Patch Management processes to ensure Company systems and infrastructure have applicable patches applied.

b. Vulnerability Management. Company shall maintain formal processes to detect, identify, report, respond to, mitigate, and remediate Security Vulnerabilities in a timely manner. As used herein, "Security Vulnerability" means a vulnerability to Company's systems or infrastructure that allows for but has not resulted in direct unauthorized access to Client Data or Client systems. Company will conduct scanning for risks, and review risks and then prioritize such risks based on Company's internal policies and procedures. Company, or a designated third-party, shall perform security assessments of Company systems and infrastructure no less than annually.

c. Security Training. Company shall instruct its personnel on industry standard security practices and applicable privacy laws and regulations and their responsibilities for protecting Client Data, no less than annually. Company shall maintain sanction standards to address violations of Company's internal security requirements or the requirements of this ISP.

d. Physical Security. Company shall establish appropriate physical security controls to prevent unauthorized physical access to Company systems and infrastructure and areas in which Client Data is stored or processed. Where practicable, this shall include controls to physically protect hardware (e.g., lockdown devices). Company shall maintain written policies and procedures which documents such controls.

7) Client Data and Communications Security

a. Exchange of Client Data. Company shall utilize a method of transmitting Client Data electronically that protects against the unauthorized access to and/or modification of such information.

b. Encryption. Company shall ensure that all Client Data whether stored (i.e., "data at rest") or that Company transmitted (i.e., "data in motion") over the public internet is encrypted using industry standard encryption processes.

c. Protection of Systems, Devices and Storage Media. Company shall establish reasonable, industry standard measures to physically secure Company systems and infrastructure to prevent any unauthorized disclosure while in transit and while at rest. Company shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of Company systems and infrastructure.

d. Data Integrity. Company shall maintain processes to prevent unauthorized or inappropriate modification of Client Data, for both data in transit and data at rest.

8) Access Control

a. Account Administration. Company shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Company systems and infrastructure and Client Data.

b. Access to Company Systems and Infrastructure. Company shall maintain appropriate access control mechanisms to prevent access to Client Data and/or Company systems and infrastructure, except by (a) specified users expressly authorized by Client and (b) Company personnel who have a need to access to perform a particular function in support of Company providing Services contracted for in the Master Agreement. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions.

c. Access to Client Systems. To the extent Company has access to Client systems, all access by Company personnel to Client systems shall be subject to prior approval by Client.

d. Backdoors. Company certifies: (1) it has not purposefully created Backdoors or similar programming that could be used to access the system and/or Client Data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to Client Data or Client systems for purposes other than providing Services, and (3) that national law or government policy does not require Company to create or maintain Backdoors or to facilitate access to Client Data or Client systems or for the Company to be in possession or to hand over the encryption key.

e. Multi-Factor Authentication Requirements. Access by Company and its employees to Client Data or any Company systems and infrastructure shall utilize Multi-Factor Authentication (MFA), or another appropriate authentication technique approved by Company.

f. Disconnecting Access. Company reserves the right to disconnect or block Client's access to the Company systems and infrastructure without notice; if such disconnection is required to protect the security, confidentiality, or integrity of Client Data and/or Company systems and infrastructure.

9) Client General Requirements

a. Account Management. Client is responsible for their accounts and third-party accounts. Usage of unique accounts, access changes and terminations, least privilege, along with complex secrets are the responsibility of Client when accessing and utilizing Company systems and infrastructure. Client acknowledges that the usage of generic or shared accounts for application access is strictly prohibited.

b. Asset Management. Client is responsible for the management and protection of any Client assets, accounts and traffic that could connect to any Company systems and infrastructure. Client is responsible for ensuring that unauthorized traffic is unable to egress/traverse in an unauthorized manner.

c. Security Assessment. Client is responsible for conducting regular security assessments and audits of their own managed devices, networks and systems not managed by Company that connect to or access Company systems and infrastructure to identify and address any potential vulnerabilities or risks.

d. Service Providers. Client is responsible for ensuring that any third-party service providers or vendors that it uses to connect to or access Company systems and infrastructure must comply with applicable laws, regulations, standards, and contractual obligations related to information security and privacy. Client shall ensure these third-party service providers and vendors have appropriate security policies and procedures in place to protect Company systems and infrastructure from unauthorized access, disclosure, modification, or destruction.

e. Auditing and Monitoring. Client is responsible, when applicable, to monitor activities and events associated with access, modification, deletion, transmission, or disclosure of electronic health records.

f. Traffic. Client shall design, develop, and maintain network and local security policies that restrict and control the inbound and outbound traffic between Client's systems and Company systems and infrastructure, as well as any other unauthorized traffic from the internet or other sources, based on the source, destination, protocol, port, or content of the packets. These policies should provide reasonable assurances to prevent any malicious or unwanted traffic from accessing or passing through Company systems and infrastructure.

g. Communication. Client is responsible for signing up for and configuring notification frequency of communications from Company to Client through the Success Community for information related to or pertaining to outage, product updates, scheduled downtimes, or other critical information that is provided to Client by the Company concerning its products and services.

h. Reporting. Client is responsible for reporting to Company any security incidents where there is reason to believe that based on the current configuration, access, or persistence of connection that Company would need to institute technical safeguards to prevent the potential of impact to Company as soon as possible and cooperate with the Company's investigation and remediation efforts.