Department of Health (DOH) Third-Party Security Requirements

The Third-Party must comply fully with all New York State (NYS) security policies and standards, as well as with all applicable State and federal requirements, in performance of the signed contract. All activity covered by the contract with DOH must be fully secured and protected by satisfactory security arrangements approved by the New York State (NYS) Department of Health (DOH).

Within the context of this security and privacy requirement document, a third party is defined as any external organization collaborating with the Department of Health (DOH) on technical solutions or data sharing. This includes, but isn't limited to, vendors, service providers, suppliers, partners, contractors, subcontractors, data processors, and data brokers.

Below are some of highlighted security requirements from the NYS and DOH policies and standards.

1) Security Governance:
    a) Security Management Team: Establish a security point of contact and collaborate with DOH and/or ITS security SMEs.
    b) Security Plan: Develop and implement a Security, Privacy and Confidentiality Plan within the first 30 days of the contract to be approved by the DOH and for all subsequent projects and major system enhancements to address security and privacy issues/risks and the steps that the Third-Party has taken to ensure these issues/risks will not compromise DOH operations. The plan shall adhere to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, moderate impact security controls and should include, at a minimum, the technical, administrative and physical

security controls listed below sections to ensure confidentiality, integrity and availability of the systems / applications.

c) Duration: Be responsible for security and privacy controls, monitoring and testing through the term of this contract.

2) Relevant Regulations and Standards: Compliant with all applicable data security and privacy regulations, including but not limited to:
   a) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and associated regulations
      i) https://www.hhs.gov/sites/default/files/privacysummary.pdf
   b) The Privacy Act of 1974
   c) New York State Statewide Technology Policies and Guidelines
      i) http://its.ny.gov/eiso/policies/security
   d) New York State Incident Breach Notification Policy
      i) https://its.ny.gov/incident-reporting
      ii) https://its.ny.gov/breach-notification
   e) National Institute of Standards and Technology (NIST) SP 800 series.
3) Data Protection:
   a) Data Encryption: Require encryption of sensitive data both in transit and at rest, utilizing FIPS approved encryption that meets the NYS Encryption Standard and secure key management practices.
   b) Data Retention Policies: Specify data retention periods, outlining how data is stored, accessed, and eventually disposed of securely as in accordance with the NYS Sanitization Secure Disposal Standard.
   c) Data Classification/Information Classification: Require proper data classification based on sensitivity levels in accordance with the NYS Information Classification Standard and implement appropriate security measures accordingly.

d) Data Residency and Sovereignty: All data, including backup data, must reside and subject to laws and regulations within the Continental United States (CONUS).

e) Data Loss Prevention (DLP): Implement DLP features to prevent sensitive data from leaving authorized boundaries.

f) Physical Security: Incorporate requirements for physical security of data storage locations and facilities, including access controls, monitoring, and environmental controls, to prevent and detect unauthorized physical access and ensure only authorized personnel can access the infrastructure and systems.

g) Unauthorized Release: Strictly prohibited from releasing or using data or information for any purposes other than those purposes specifically authorized by NYS DOH and specified within the contract.

4) Access Control and Authentication:

a) Multi-Factor Authentication: Implement multi-factor authentication (MFA) for internal and external users, including development and operational access. For service accounts utilize strong risk-based authentication methods in accordance with the NYS Authentication Tokens Standard and Digital Identity Policy and Standard.

b) Authentication Method: Integrate with DOH supported authentication solutions, Health Commerce System (HCS) and/or NY.gov ID authentication mechanism and be accessible through the Department of Health's web portal, Health Commerce System (HCS) or NY.gov ID.

c) Access Control Levels: Define granular permission levels to prevent and detect unauthorized or inappropriate access and ensure that authorized users and service accounts only have access to the information they need to

perform business duties assigned to them with appropriate access controls by employing least-privilege and role-based access.

d) Role-based Access Control: Roles shall be definable without changes to the software: E.g. Allow a security administrator to assign user roles. Allow multiple roles to be assigned to any user. Allow users roles to be assigned locally by local System Administrators with local System Administrator access privileges.

e) Geolocation-based Restriction: Access should be restricted to Continental United States (CONUS) only for all privileged accounts, developers and support staff members.

f) Restricted Access: Ensure that access to systems and information is restricted to authorized users. Assure the privacy of data captured for current and prior clients, providers, and others that store confidential information in the database. Restrict access to its data, based on roles defined in the system, e.g. ensure that providers cannot see information about any providers other than themselves and allow only designated Database Administrators (DBAs) to view database level data storage.

g) Password Management: Passwords shall be able to be reset by the DOH System Administrator. User passwords shall not be viewable to anyone, even Database Administrators. Passwords shall be able to be reset by a security administrator. All reset passwords shall require immediate change by the user upon next logon.

h) Account Termination: Access to terminated, unauthorized or inactive users shall be disabled immediately in accordance with the NYS Account Management/Access Control Standard.

i) Periodic User Access Review: Periodically review and confirm that all active users are still authorized and associated with the authorized program.

5) Configuration and Change Management:
    a) Configuration Change: Configuration changes must be analyzed for security impact, tested, and approved prior to implementation in accordance with the NYS Secure Configuration Standard.
    b) Change Management: Have proper change management process and procedure in place to prevent unauthorized system, configuration and/or code changes.
6) Vulnerability Management:
    a) Vulnerability Scanning: Perform regular vulnerability scanning to identify and remediate and/or mitigate security weaknesses in accordance with the NYS Vulnerability Management Standard.
    b) Vulnerability Reporting: Provide periodic report on vulnerability management status and POA&M for all outstanding vulnerabilities.
    c) Patch Management: Apply security related software or firmware updates (patches) to applicable IT systems in a timely manner as in accordance with the NYS Patch Management Standard.
7) Security Audits and Testing:
    a) Security Risk Assessment: Undergo regular security risk assessments and audits, preferably performed by an independent qualified third-party security contractor, to demonstrate adherence to security regulations and standards. Issues identified in the security risk assessment must be addressed with a plan for resolution and resolved within a reasonable timeframe in accordance with the NYS Information Security Risk Management Standard.
    b) SOC 2 or Other Audits or Security Assessment: Periodically provide reports of security audits conducted by a third-party, such as a SOC 2 Type 2 report.

c) Penetration Testing: Perform penetration testing annually to identify and remediate and/or mitigate vulnerabilities in the systems and applications, preferably by an independent qualified third-party security contractor.

8) Secure Software Development Lifecycle (SSDLC):
   a) Secure Coding Standards: Adhere to secure coding standards and best practices during application development in accordance with the NYS Secure Coding Standard.
   b) Code Reviews: Perform code reviews, static and dynamic code analysis and testing to identify and address security vulnerabilities prior to release into the production environment. The use of a Development / QA environment for such testing is expected and must not store authentication credentials or sensitive data in its source code.
   c) SSDLC Processes: Follow secure software development lifecycle (SSDLC) processes, including policies, training, audits, and testing, in accordance with the NYS Secure System Development Life Cycle Standard.
9) Logging and Monitoring:
   a) Audit Logs: All necessary audit trails for all data transmission, access and processing activities must be implemented and monitored regularly to identify unauthorized or inappropriate access to any device or service within the network, suspicious network scans or other anomalies, in accordance with the NYS Security Logging Standard.
   b) Access Control Logging: Actively log and monitor all user access, actions and activities to systems, applications, and data, including the specific permissions granted and any modifications made and access to privileged accounts and sensitive data.
   c) Log Data Capture: Capture all relevant data elements in logs, including but not limited to: Access date and time, Username attempting access, Success

or failure of access, Source of access, Target of access. Information should be provided to NYSDOH upon request.

d) Log Retention: Logs must be retained, stored and protected in accordance with the NYS Security Logging Standard and relevant regulations.

e) Security Monitoring and Alerting: Perform real-time security monitoring and alerting for suspicious activities, interruption or disaster must be implemented and maintained.

10) Business Continuity and Disaster Recovery:

a) Backup: Data must be backed up and maintained off-site. The backup data must be tested periodically.

11) Incident Response:

a) Notification Procedures: Have clear notification procedures in place for reporting security incidents, including potential breaches. Notification should at a minimum include the root cause and method(s) of resolution of the security issue.

b) Incident Response Plans: Have a detailed incident response plan that outlines the steps the vendor will take to address security incidents in accordance with the NYS Cyber Incident Response Standard.

c) Timely Incident Reporting: All material incidents, including significant third-party or supply chain incidents impacting the NYSDOH, must be reported immediately to NYSDOH and NYS ITS upon becoming aware of the occurrence and no later than 24 hours.

d) Emergency Preparedness: Recovery procedures, in the event of a business interruption or disaster, must be implemented and maintained.

12) Data Breach Notification:

a) Timely Breach Reporting: Notify the DOH immediately, and no later than 24 hours, of any breach of security, privacy and confidentiality, as well as

comply with any federal or State laws or regulations related to other notification in relation to such breach.

b) Notification Procedures: Define clear procedures for notifying affected individuals and relevant authorities in the event of a data breach.

c) Data Breach Response Plan: Outline the steps it will take to contain and mitigate the impact of a data breach.

13) Third-Party Security Risk Management:

a) 3rd Party Risk Management Process: Have in place a process of identifying, assessing, and mitigating risks associated with external parties, including vendors, suppliers, and partners.

14) Artificial Intelligence (AI):

a) Responsible AI Adoption: Manage AI security risks in accordance with the NYS Acceptable Use of Artificial Intelligence Technologies Standard to ensure the safety, reliability, and trustworthiness of the usage of the AI systems.

15) Privacy:

a) Data Minimization: Only collect and retain PII that is strictly necessary for the specified purpose of the software.

b) Privacy by Design and by Default: Commit to privacy by design principles, ensuring that privacy considerations are integrated into the software development process from the outset, and privacy by default, meaning the most privacy-protective settings are the default.

c) Data Sharing with Third-Party: Must not, without written authorization from the DOH, divulge to other third parties any confidential information obtained by the Third-Party or its agents, distributors, resellers, subcontractors, officers or employees during the course of performing contract work. This information includes, but is not limited to security procedures, business

operations information or commercial proprietary information in the possession of the DOH, Protected Health Information (PHI) or other data. In addition, a HIPAA Business Associate Agreement (BAA) is required.

d) Confidentiality: Treat all information obtained through its performance under the contract as confidential information and will not use any information so obtained in any manner except as necessary for the proper discharge of its obligations and securing of its rights, or as otherwise provided. State or federal officials, or representatives of these parties as authorized by State or federal law or regulations, will have access to all confidential information in accordance with the requirements of State and federal laws and regulations.

e) DOH Authority: The DOH will have absolute authority to determine if, and when, any other party may be allowed to access information. Confidentiality is the concept that data will be viewable only by those who are explicitly permitted to view it.

f) User Agreement: The system must include a clearly defined user agreement to ensure users are aware of and consent to the privacy policy upon log-in and before interacting with data. There must be an ability to update the user agreement to reflect changes in regulations, policies and legal requirements.

16) Overall Security and Privacy Posture:

a) Security Team and Expertise: Have sufficient size and expertise of their security and privacy teams.

b) Security Policies and Procedures: Provide copies or summaries of their key security and privacy policies and procedures upon request.

c) Right to Audit: NYSDOH has the right to audit the Third-Party security and privacy practices.

d) Staff Education: Take steps to ensure that their staff, agents and subcontractors are educated in specific security, privacy and confidentiality requirements as applied to this contract, explaining its responsibilities in maintaining security, privacy and confidentiality and reviewing all policies, processes and procedures that will be used for this project.

e) Training: Provide training to DOH and Third-Party staff on the Third-Party's privacy and security procedures, which should comply with the State and Federal requirements for security privacy.