APPENDIX C - INFORMATION SECURITY REQUIREMENTS
Health Maintenance Organizations
Specifications for the NYSHIP

New York State Department of Civil Service
August 2024

The following requirements shall be effective as of the date the Contractor or Contractor Staff first receives, maintains, transmits, accesses or otherwise comes into contact with Confidential Information. These requirements are intended to describe the minimum standard for physical, technical and administrative controls affecting Confidential Information in relation to the Services being provided under the Agreement.

The Department may suspend access to Department Systems or Data at any time if the Department, in its sole discretion, believes Contractor is not complying with any of its obligations herein.

Definitions

All capitalized terms herein shall have the meaning as set forth in this Appendix. If not defined herein will have the meaning as set forth in the resulting Contract including the Appendices and Attachments thereto, or if not defined therein will have the meaning as defined in 45 C.F.R. Parts 160-164.

Application means a program or group of programs designed for end users.

Authorization means access privileges granted to a user, program, or process or the act of granting those privileges.

Availability means the extent to which information is operational, accessible, functional, and usable upon demand by an authorized entity (e.g., a system or user).

Cloud Service means any Product or Service sold as an “as a service” offering and has one or more of the following characteristics:

(a) User Data is transmitted, acted upon, or stored on equipment not owned by the User;

(b) Allows a Contractor access to User Data from a location other than the User’s premises; or

(c) Allows a user access to data not owned by the User which access may or may not result in the collection of User Data. (see also Hosted Application)

Event means Any observable occurrence in a system and/or network that may indicate than a Security Incident is occurring or has occurred.

Firewall means a system designed to prevent unauthorized access to or from a private network based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both.

Hardware means tangible objects such as disks, disk drives, display screens, keyboards, printers and chips http://www.webopedia.com/TERM/h/disk.html.

Hosted Application means a software as a service (SaaS) solution that allows users to execute and operate a software application entirely from the cloud on a recurring subscription basis.

- A Hosted Application is hosted and powered from the remote cloud infrastructure and are accessed globally through the Internet. It provides the same functionality as locally installed software but can be updated more easily.

- A Hosted Application may also be known as Internet-based application, Web application and online application.

Network means multiple devices (e.g. computers) that are linked or communicate with one another.

Security Incident means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A Security Incident is also defined as any Event that adversely affects the confidentiality, integrity, or Availability of a System and its Data. See NYS ITS Policy NYS-S13-005 or its successor for additional information.

Virus means any computer code, whether or not written or conceived by Contractor, that disrupts, disables, harms, or otherwise impedes in any manner the operation of the Product, or any other associated software, firmware, hardware, or computer system (such as local area or wide-area networks), including aesthetic disruptions or distortions, but does not include security keys or other such devices installed by Product manufacturer. Virus shall also include any malware, adware, or other computer code, whether or not written or conceived by Contractor, that allows data or metrics to be copied, redirected, or modified without the express consent of DCS.

1. Compliance

Contractor agrees to preserve the confidentiality, integrity and accessibility of Data with administrative, technical and physical measures that conform to federal, State and

Department mandates, and the security controls as stated herein, based upon the nature of the Project Services provided, the Data involved, and/or the location where such Project Services are provided. Accordingly, Contractor warrants, covenants and represents that it shall fully comply with all New York State Information Technology Cybersecurity Policies, Standards and Procedures published by the New York State Chief Information Security Office at https://its.ny.gov/policies, as amended from time to time, that are applicable to the Project Services being provided by Contractor. Contractor is responsible for understanding which policies and state or federal laws apply to the Project Services and the Data in scope for the Agreement. The Department is required to provide a minimum of thirty (30) days written notice to the Contractor of changes to policies or rules under this section. If the requirements set forth herein are not the same as the New York State enterprise security policy, standard or procedures, then the more restrictive requirement applies. Contractor is responsible for assessing and monitoring Subcontractor control environments for compliance with the standards as documented herein. The Department reserves the right to immediately revoke system or access privileges where such privileges pose an undue risk to the State.

2. Acceptable Use of Information Technology Resources

Contractor, including all Contractor Staff, accessing the State's Information Technology Resources in the course of their work for the Department are required to comply with New York State Information Technology Policy NYS-P14-001 – Acceptable Use of Information Technology Resources, as amended from time to time, prior to accessing any New York State Information Technology resources.

Access to the State's Networks, Systems, Data, or Facilities is provided to support the official business of the Department. Any use inconsistent with the Department's business activities and administrative objectives is considered unacceptable or inappropriate use.

The Department reserves the right to change its policies and rules at any time, with regard to the acceptable use of Department Networks, Systems, Data or Facilities. Non-compliance with these provisions or unacceptable use of Department Networks, Systems or Facilities may result in the revocation of system privileges, termination of the Agreement with Department, and/or criminal and/or civil penalties.

3. Information Security Program

3.1 Contractor must maintain a written Information Security Program ("WISP") including documented policies, standards, and operational practices that meet or exceed the requirements and controls set forth herein to the extent applicable to the Project Services and identify an individual within the organization responsible for its enforcement. Contractor's WISP shall address, at a minimum, all security requirements

as listed in these requirements, as amended from time to time, and comply with all state and federal data security and privacy laws applicable to the Department. This documentation will be reviewed by Contractor's security official, or its designee, at least annually and shall be updated periodically with changes to organization, technology, or Services. When implementing security controls Contractor shall take a risk-based approach. Any control exceptions which represent risk will be formally documented, monitored, and periodically reviewed.

3.2 Upon request by the Department, Contractor's WISP shall be made available to and reviewed by the Department or the Department's representative. At the Department's request and at no cost to the Department, Contractor shall make mutually agreed upon, commercially reasonable modifications to its WISP or to its data security controls in order to conform to the requirements set forth herein. The Department reserves the right, in its sole discretion, to terminate Contractor's access to Confidential Information until such time as Contractor has made such modifications to its WISP or data security controls. Contractor shall notify the Department in writing of any changes to systems, facilities or WISP controls affecting Confidential Information. This notification should set forth in detail how such changes will impact the Confidential Information.

3.3 Contractor shall apply appropriate sanctions against Contractor Staff who fail to comply with security policies and procedures.

3.4 Contractor shall have processes and procedures in place so that Security Incidents will be reported through appropriate communications channels as quickly as possible. Contractor shall periodically test, review, and update such processes and procedures. All Contractor Staff shall be made aware of their responsibility to report any Events prior to being granted access to any Confidential Information. If at any time during the Agreement, Contractor becomes aware of an Event or that it or any of its Subcontractors will or do not meet the obligations described within these requirements, Contractor will immediately notify the Department.

3.5 Contractor shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and Availability of Confidential Information. The assessment must be reviewed by Contractor's security official and used to inform the Contractor's information security program.

3.6 Upon request, the Contractor shall identify to the Department the security official who is responsible for the development and implementation of the Contractor's policies and procedures.

4. Right to Assess, Audit and Certify

4.1 The Department, or its designated agents, may assess or audit the effectiveness of Contractor's compliance with requirements herein. The Department shall provide advanced notice of any assessment or audit. The Parties shall mutually agree in writing to the timing of the assessment or audit.

4.2 Upon request, Contractor shall complete a security controls assessment conducted by the Department or its designated agent ("Security Assessment"). To the extent that the security controls assessment identifies any risks or deficiencies for which remediation is required, such remediation requirements or compensating controls (and the timeframes within which the remediation requirement or compensating control must be successfully implemented) will be provided in writing to the Contractor. The Department and Contractor agree to negotiate in good faith a mutually agreeable timeframe within which the remediation requirements or compensation controls must be successfully implemented. If an agreement cannot be had, the Department will make the final determination regarding the timeframe. Contractor's failure to complete any remediation requirements within the required timeframe shall be deemed to be a material breach of the Agreement.

Where the Contractor is a Business Associate, or hosts, maintains or has access to Department Protected Health Information, certification in the HITRUST Common Security Framework (CSF) is required. The Department, in its discretion, may accept a comparable industry accepted security assessment certification in lieu of a HITRUST Common Security Framework (CSF) certification. (For purposes of these requirements a SOC 2 attestation report is deemed a comparable industry accepted assessment.) If an alternative security assessment certification is accepted, then such alternative certification shall replace the following references to HITRUST.

4.2.1 If the Contractor has a HITRUST CSF Certification applicable to the Project Services and/or applications in scope for the Agreement as of the Effective Date of the Agreement and maintains it throughout the Agreement, then that HITRUST CSF certification, at the discretion of the Department, will be accepted in lieu of a security controls assessment identified in Section 4.2. Documentary evidence for HITRUST CSF certification must be provided to Department upon request and include, at a minimum, sections of the HITRUST CSF report that demonstrate Contractor's scoring across all domains and any corrective

action plans required as a condition of certification. Upon Contractor's written request, the Department shall return all such documentary evidence to Contractor. The Department may ask questions related to the protection of Confidential Information after review of documentation supporting the HITRUST CSF Certification. The Contractor's HITRUST CSF Certification does not waive Department's rights to assess under Section 4.1 herein or other audit rights, including rights to onsite facility inspection, provided elsewhere in the Agreement.

4.2.2 If the Contractor is without a HITRUST CSF certification or an approved alternative security assessment certification as of the Effective Date of the Agreement, Contractor shall:

- Complete and provide to the Department a HITRUST CSF Self-Assessment Report no later than 90 days after the Effective Date of the Agreement; and
- Obtain and provide to the Department a HITRUST CSF Validated Report no later than 18 months after the Effective Date of the Agreement; and
- Obtain and provide to the Department a HITRUST CSF certification and associated documentation, including but not limited to complete validated reports and corrective action plans, no later than 24 months after the Effective Date of the Agreement.

4.2.3 If Contractor has begun the process of obtaining a HITRUST CSF Certification before the Effective Date of the Agreement, then Contractor represents and warrants to the Department that all corrective action plans that are necessary to obtain a HITRUST CSF Validated Report and/or HITRUST CSF Certification and that have been identified to Contractor prior to the Effective Date shall be communicated to the Department and documented in writing to the Department.

4.2.4 Within 30 days of identification, the Contractor shall report to the Department any findings through the HITRUST engagement that materially impacts Confidential Information. In addition, the Contractor will provide the associated corrective action plans identified during any self-assessment or third-party assessment, including any

assessment related to Contractor's independent certification/attestation. Contractor will provide the Department with any further Information associated with such findings, as reasonably requested by the Department. Upon Contractor's written request, the Department shall return all such documentary evidence to Contractor.

4.2.5 If at any time during the Agreement, the CSF Certification is withdrawn for any reason, Contractor will contact the Department within 24 hours of learning of the issue to provide information and remediation plans regarding the withdrawal.

4.3 From time-to-time Contractor may be requested to respond to, inform and provide updates regarding specific high-risk security gaps or exposures that exist for new or emerging security vulnerabilities that are made publicly known for systems, applications, hardware devices, etc. In all instances Contractor will provide a response to any Department inquiry within five business days and will provide specific details as to the questions asked to ensure that the Department can appropriately evaluate the risk or exposure to the Confidential Information while still protecting the systems, applications, hardware devices etc. from further vulnerabilities.

5. Encryption

5.1 Contractor shall apply encryption methodology that, at minimum, conforms to the Federal Information Processing Standards Publication 140-3 Security Requirements for Cryptographic Modules and applicable state and federal regulations ("Approved Encryption").

5.2 Cryptographic key management procedures must be documented and include references to key lifecycle management (including provisioning, distribution, and revocation) and key expiration dates.

5.3 Access to encryption keys must be restricted to named administrators. Encryption keys must be protected in storage. For example, methods of acceptable key storage include encrypting keys or storing encryption keys within a hardware security module (HSM). Data-encrypting keys should not be stored on the same systems that perform encryption/decryption operations.

5.4 Except as otherwise agreed to in writing by the Contractor and Department, Confidential Information must be encrypted while in transit and at rest across at least the following types of assets:

- Public shared Networks
- Non-wired Networks
- Cloud Services
- Desktop and portable computing devices
- Mobile devices
- Portable media
- Back-ups
- Application or Network servers
- ‘Plug & play’ storage devices

6. Network and Systems Security

6.1 Contractor shall utilize and maintain a commercially available, industry standard malware detection program which includes an automatic update function to ensure detection of new malware threats.

6.2 Contractor shall maintain an intrusion detection or prevention system that detects and/or prevents unauthorized activity traversing the Network.

6.3 Contractor shall have technical controls to detect, alert, and prevent the unauthorized movement of Data from Contractor’s control (commonly referred to as Data Loss Prevention).

6.4 Networks or applications that contain Confidential Information must be separated from public Networks by a firewall to prevent unauthorized access from the public Network.

6.5 At managed interfaces, Network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).

6.6 Contractor shall establish security and hardening standards for Network devices, including Firewalls, Switches, Routers, Servers, and Wireless Access Points (baseline configuration, patching, passwords, and access control).

6.7 Web content filtering must be in place to restrict external webmail, instant messaging, file sharing and other Data leak vectors for any Contractor Staff with direct or indirect access to Confidential Information.

6.8 Quarterly (unless the System has an Impact Risk rating of High* in which case monthly) vulnerability scans must be performed, and intrusion detection and identity management systems must be installed and monitored on all systems and components that handle, process, or store Confidential Information. Upon request, report summaries must be

provided to the Department, including confirmation of remediation for vulnerabilities identified as high- or medium-risk (or equivalent classifications). *See NYS-S15-002 Vulnerability Management Standard.

6.9 At a minimum, Contractor shall engage a qualified third party to perform annual penetration testing of Contractor's Networks containing Confidential Information. The scope of the penetration testing must, at a minimum, include all internal/external systems, devices and applications that are used to process, store, or transmit Confidential Data. Contractor must provide the Department with summary results and a remediation plan at the Department's request.

6.10 If Contractor provides products or Services related to the Agreement through a Department portal or mobile applications, especially those which are internet-facing, or use Department domains, the Department's portal, mobile applications and domain are subject to Department scanning and assessments. Contractor agrees to remediate vulnerabilities identified during this process in a manner and timeline acceptable to the Department.

6.11 Contractor shall ensure that no unencrypted Confidential Information is stored in any system that is internet facing.

6.12 Contractor shall use secure means (i.e., HTTPS, FTPS) for all electronic transmission or exchange of System, user and application information with the Department.

7. Mobile Device Security Controls

7.1 Contractor must have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and security requirements for all mobile devices.

7.2 Where Contractor permits Bring Your Own Device (BYOD), Contractor must have a BYOD policy that defines the device and eligibility requirements for BYOD usage in the event that Confidential Information will be viewed or stored on devices that are not Contractor-issued mobile devices.

7.3 Contractor must post and communicate the mobile device policy and requirements through Contractor's security awareness and training program.

7.4 Contractor must have a centralized mobile device management solution (MDM) deployed to all mobile devices that are permitted to store, transmit, or process Confidential Information.

7.5 Contractor's mobile device policy must require the use of encryption for either the entire device or for Confidential Information and must be enforceable through Contractor's MDM solution or other technical controls.

7.6 Contractor must enforce password policies for Contractor-issued mobile devices and/or BYOD mobile devices using Contractor's MDM solution or other technical controls.

7.7 Contractor's Information Technology department must provide remote wipe or corporate Data wipe for all mobile devices in the event that Confidential Information will be viewed or stored on mobile devices.

8. System and Application Controls

8.1 All Confidential Information must be securely stored at all times to prevent loss and unauthorized access or disclosure.

8.2 Laptop and workstation systems that access Confidential Information remotely must utilize endpoint protection which includes a personal firewall and anti-malware protection.

8.3 Operating systems and application software used must be currently supported by the manufacturer.

8.4 Current versions of operating system and application software must be maintained, and patches applied in a timely manner for all systems and applications that receive, maintain, process, or otherwise access Confidential Information.

8.5 Confidential Information must not be used in any non-production environment such as testing or quality assurance unless de-identification of the Data has been performed. In the event that de-identification is not practical or feasible, compensating controls must be in place protecting the Data to the same level of protection as afforded to the production environment. Confidential Information must not be placed into a nonproduction cloud computing environment unless deidentified or compensating controls are in place protecting the Data to the same level of protection as afforded to the production environment.

8.6 Confidential Information must be segmented from non-Department Information so that appropriate controls are in place to identify the Data

as Department's in all instances, including backup and removable media, and to appropriately restrict access only to users authorized to view the Data. Logical separation must allow Data to be deleted when it is no longer required.

8.7 Logical controls, virtual machine zoning, virtualization security and segregation must be in place to help prevent attacks and exposure in multi-tenancy environments containing Confidential Information.

8.8 Contractor shall maintain an asset management system which records the movement of hardware and electronic media and any persons responsible, therefore.

9. Software Development Lifecycle

9.1 Contractor must use industry standards such as BSIMM, NIST, OWASP, etc. to build in security for its Systems Development Lifecycle (SDLC). See also NYS-S13-001 for further information on the SDLC requirements at its.ny.gov/document/secure-systemdevelopment-life-cycle-ssdlc-standard.

9.2 Contractor must use both an automated and manual source code analysis tool to detect and remediate security defects in code prior to production deployment.

9.3 Contractor must have policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for the Project Services it provides to Department.

9.4 Contractor must have controls in place to prevent unauthorized access to its or Department's application, program, or object source code and ensure that access is restricted to authorized personnel only.

9.5 National identifiers or Social Security Numbers must not be utilized as User IDs for logon to applications.

10. Physical Controls for the Protection of Confidential Information

10.1 All Confidential Information received or created in paper form must be protected from viewing by unauthorized persons.

10.2 A clean desk policy will be enforced to ensure proper safeguarding of all hard copy Confidential Information.

10.3 Visitor logs documenting all individuals who are not Contractor Staff who gain access to the facility where Confidential Information is processed will be maintained.

10.4 Confidential Information shall not leave control of the Contractor without the written approval of Department.

10.5 Servers, enterprise data storage devices, backup tapes and media, and other computing devices that contain Confidential Information used to support Network communications must be located in a secure and restricted access location.

10.6 Monitoring cameras (e.g., CCTVs) must monitor ingress and egress to sensitive areas within the facility. The monitoring equipment (e.g., CCTV) feed must be monitored either internally or externally by a qualified team. Alerting procedures must be defined and notification performed to qualified Contractor personnel. Processes for retention and review of security logs (e.g., access and visitor logs, CCTV) must be in place. Cameras must be positioned in a way that Confidential Information is not readable on screens and/or on CCTV recordings or screen captures.

10.7 When investigation of an incident or Breach is required, summary reports related to the incident or Breach and all audit trails and CCTV recordings shall be made available to Department upon request and in a timely manner. Upon Contractor's written request, the Department shall return all such documentary evidence to Contractor.

11. Access Control

11.1 Prior to gaining access to Confidential Information, Contractor Staff will have appropriate background checks completed in compliance with state and federal law. See Standard Clauses for All Department Contracts (Appendix B), Onboarding and Suitability Determinations.

11.2 Security awareness training will be completed by Contractor Staff prior to access being granted to Confidential Information, and then completed on an annual basis going forward so long as access to Confidential Information continues. This training should include, at a minimum, guidance on defending against malware, protecting passwords, monitoring and reporting system notifications, social engineering, and handling sensitive Data. The Department may require Contractor Staff to complete Department specific security training at no additional cost to the Department.

11.3 Physical and logical access will be granted to the minimum Confidential Information necessary to meet the requirements of the user's scope of responsibilities.

11.4 Access reviews will be performed at least quarterly for privileged user accounts and at least annually for non- privileged user accounts. The Department reserves the right to request the Contractor to perform an additional access review for non-privileged user accounts if there is evidence of inappropriate access.

11.5 Only those individuals providing Project Services to the Department, or those who are responsible for administering or managing systems that contain Confidential Information, shall be authorized to access systems containing Confidential Information.

11.6 All Contractor Staff that are no longer required or authorized to access Confidential Information or systems that contain Confidential Information must have access promptly disabled.

11.7 Access to Confidential Information and systems that contain Confidential Information must be access controlled through the use of individual user IDs and passwords that substantially meet the NYS Authentication Tokens Standard NYS-S14-006 standard complexity rules and password lifetimes.

11.8 If it is suspected that a password has been compromised, the password must be immediately changed or reset.

11.9 Processes must be in place to create audit trails capable of determining who has accessed Confidential Information and/or systems that contain Confidential Information.

11.10 Remote access to systems or Networks that contain Confidential Information must use multi-factor authentication and a connection with Approved Encryption as defined in Section 5 above.

11.11 The Department reserves the right to immediately terminate remote access connections to Department or State Networks and Systems.

11.12 Upon request, Contractor shall provide reports within 48 hours for:

11.12.1 List of all individuals with access to Confidential Information and/or systems that contain Confidential Information and the level of access granted;

11.12.2 List of activity associated with any user ID who has access to Confidential Information; and

11.12.3 Account management capabilities, such as account lockouts for unsuccessful logon attempts, defined inactivity times, remote access allowances, specific success and failure events, and management of elevated privilege accounts must be enforced.

11.13 All identity credentialing, authentication, Authorization, and access control events must be logged, and those logs are subject to periodic audit by the Department. At a minimum, the logs of all specified success and failure events associated with identity and access management in the computing environment it manages must be produced. These logs must then be archived for at least twelve months. These archived logs must be searchable and or discoverable. Contractor may redact information regarding those individuals who do not have access to the Department's data.

12. Data Protection

Contractor must protect Confidential Information from unauthorized access, use, alternation, disclosure, or dissemination. The Contractor must, in accordance with applicable law and the instructions of the Department, maintain such Data for the time period required by applicable law, exercise due care for the protection of Data, and maintain appropriate data integrity safeguards against the deletion or alteration of such Data. If any Data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of this Contract, then Contractor shall, at its own expense, use its best efforts to reconstruct such Data as soon as feasible. In such event, Contractor shall reimburse the Department for any costs incurred by the Department in correcting, recreating, restoring or reprocessing such Data or in providing assistance therewith.

13. Physical Data Transport

The Contractor shall use, if applicable, reputable means to physically transport Data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This requirement applies to transport between the Contractor's offices, to and from Subcontractors, and to the Department.

14. Data Return and Destruction

At the expiration or termination of the Agreement, at the Department's option, the Contractor must provide the Department with a copy of the Data, including metadata and attachments, in a mutually agreed upon, commercially standard format. The Contractor must provide the Department continued access to the Data beyond the

expiration or termination of the Agreement for the period designated in the Contract. Thereafter, except for Data required to be maintained by law or this Agreement, Contractor shall destroy Data from its systems and wipe all its data storage devices to eliminate any and all Data from Contractor's systems. The sanitization process must comply with New York State Security Policy NYS-S13-003. If immediate purging of all data storage components is not possible, the Contractor will certify that any Data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. Contractor must then certify to the Department, in writing, that it has complied with the provisions of this paragraph.

15. Offshore Security Requirement

Confidential Information, including Protected Health Information, is not permitted to be hosted, maintained, stored, processed or otherwise accessed outside CONUS (“offshore”).

16. Contingency Planning

Contractor will have documented Business Continuity and Disaster Recovery plans in place that include Information security controls. Such plans will be tested at least annually.

17. Incident Response

17.1 Contractor will have a documented Incident Response Plan. Such plan will be tested at least annually.

17.2 Incident response roles and responsibilities must be clearly outlined between Contractor and Department as appropriate.

18. Payment Card Industry Data Security Standard

If, in performing Project Services to or on behalf of Department, Contractor acts as a Merchant or payment card processor as defined by the Payment Card Industry Data Security (PCI DSS) standard, then Contractor agrees to comply with the applicable PCI DSS requirements.

19. Litigation Holds

The Contractor must provide a detailed mechanism for how litigation holds will be implemented. This description shall include how metadata will be created, accessed, and stored in a cloud environment.