Medicaid Systems Quality Assurance Services

Attachment K – Division of Operations and Systems Security and Privacy Requirements

Security and Privacy Requirements

The New York State Department of Health (the "Department" or "DOH") requires that vendors providing information technology (IT) and application services to the Department comply with the security and privacy policies and controls outlined in this RFP and all other applicable New York State and federal laws, regulations, policies, and standards for IT systems that transfer, process, or store Department data, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule. Vendors are required to verify compliance with security and privacy requirements by providing the Department with documentation and artifacts that validate applicable standards and controls are in place.

Moderate-Plus Security Controls Baseline

The Department has defined a *Moderate-Plus Security Controls Baseline* based on, and consistent with the security provisions described in Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 at the Moderate level. Additionally, the Department has augmented these federal standards with New York State Policies and Standards. The *Moderate-Plus Security Controls Baseline* includes a System Overview document. All bidders shall complete the System Overview document – which is attached to this RFP – to thoroughly and accurately describe the technical security environments that will support the proposed system.

System Security Plan (SSP)

The Department requires the selected bidder/vendor to maintain a System Security Plan (SSP) that aligns with the *Moderate-Plus Security Controls Baseline* for any system that will transfer, process, or store Department data. The Department considers bidder responses to represent a commitment by the bidder to adhere to, and demonstrate compliance with, the *Moderate-Plus Security Controls Baseline*. The Department will provide necessary templates and guidelines with respect to SSP format to the selected bidder/vendor upon contract award.

Data Use Agreement (DUA) and Business Associate Agreement (BAA)

Selected bidder/vendor shall execute a Data Use Agreement (DUA) and Business Associate Agreement (BAA) and submit a System Security Plan (SSP) Attestation to the Department upon contract award. The SSP Attestation requires the selected bidder/vendor to certify to the Department that the selected bidder/vendor system adheres to the *Moderate-Plus Security Controls Baseline*.

FedRAMP Certified Cloud Solutions

If the selected vendor solution utilizes a FedRAMP Certified cloud solution, the vendor shall indicate how such cloud services are utilized, including the type of cloud service utilized (e.g. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/ or Software as a Service (SaaS)).

Additionally, vendor shall provide a matrix that illustrates whether the vendor, or the cloud service provider, is responsible for each security control. Vendor shall also indicate if responsibility for a given control is shared between the vendor and the cloud service provider.

Selected vendor shall also provide evidence to the Department that the cloud service offerings have been certified against criteria consistent with the *Moderate-Plus Security Controls Baseline.* The scope of this certification shall include all locations that store, process, connect to, or provide access to Department data, whether at rest or in transit.

The Department reserves the right to request documentation to verify compliance with FedRAMP and FISMA Authorizations including but not limited to:

- System Security Plans
- Cloud Security Alliance ASA certification reports
- SOC audit reports
- Other independent security assessment results
- Artifacts employed in support of cloud provider certification
- Identification of cloud provider supply chain vendors and associated contracts as applicable

Department Templates

The DUA, BAA, SSP Attestation, *Moderate-Plus Security Controls Baseline* SSP templates, and POA&M templates will be provided to the selected bidder/vendor by the Department upon contract award.

Legal and Regulatory Compliance

Bidders/vendors should familiarize themselves with all applicable New York State and federal laws, regulations, policies, and standards for IT systems that transfer, process, or store Department data.

Finally, systems addressed by this RFP may be subject to security and regulatory requirements including, but not limited to:

- New York State ITS policies and standards
- The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule
- All applicable State and federal laws and regulations related to privacy protections
- NY Social Services Law (§) 367-b(4) of the
- New York State Social Services Law Section 369(4)
- Article 27-F of the New York Public Health Law (HIV/AIDS)
- 18 NYCRR 360-8.1
- NY Civil Rights 79-L
- Social Security Act, 42 USC 1396a(a)(7)
- Federal regulations at 42 CFR 431.302 and 42 CFR Part 2 (Substance Use Disorder)
- NYS Mental Hygiene Law Section 33.13
- 45 CFR Parts 160 and 164 (Privacy related sections for HIPAA)