GEORGIA DEPARTMENT OF COMMUNITY HEALTH

Medicaid Enterprise System Transformation

State of Georgia, Department of Community Health Third-Party Liability (TPL) Security Standards:

The Georgia Department of Community Health (DCH) and its service organizations (including sub-contractors) must ensure that all applicable Federal and State Security & Privacy Laws, Regulations and Standards are met for the protection of all State Data including sensitive and confidential information, prior to being allowed access to State Data. Applicable Federal Regulatory Compliance Laws include, HIPAA Privacy and Security Rules as well as, Breach Notification Laws, the Privacy Act of 1974 enacted for the protection of Personally Identifiable Information (PII), the *Electronic Government Act of 2002 (FISMA) applicable National Institute of Standards and Technology (NIST) Federal Computer Security Standards for the implementation of FISMA Federal Law, Technical System Security Requirement (TSSR) Standards as published by the Social Security Administration (SSA) and applicable State of Georgia Enterprise Information Security Policies, Standards and Guidelines (PSG's).* The following security standards are requirements are applicable to DCH Third-Party Liability Program Solutions and Services:

R1. **HIPAA Omnibus Laws, Regulations and Standards:** Contractor solutions and services shall comply with the requirements of the *Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the HITECH Act*, and all implementing regulations (together, the "*HIPAA Privacy and Security Rules*").

R2. **HIPAA Business Associate Agreement:** Contractor agrees to provide DCH with a signed HIPAA Business Associate Agreement. Contractor agrees to comply with the terms of the agreement and must ensure that its Sub-contractors and third-party service organizations comply with the terms of the agreement including applicable HIPAA Privacy, Security and Breach Notification Laws, Regulations and Standards prior to being allowed access to State Data.

R3. **Privacy & Security Awareness Training:** Contractor shall ensure that all individuals with access to State data complete Cybersecurity Awareness Training, Privacy Act of 1974 Training for the Protection of Personally Identifiable Information as well as, Social Security Administration Rules of Behavior training. This includes staff, contractors, suppliers, vendors, business partners and others. Awareness training requirements will be determined by federal laws, regulations and regulatory compliance requirements. Contractor must ensure that all staff are trained at least annually and that current training records are maintained. Awareness training criteria should address the following subject areas, at a minimum:

- Role-based Access Control
- Encryption of Stored and Transmitted PHI
- HIPAA Omnibus Laws, Regulations, and Standards
- Privacy & Security Incident Response Policy and Procedures
- Sanctions for Violations of HIPAA Privacy and Security Policies
- Privacy Act Legislation for the protection of PII and SSA Rules of Behavior

R4. **NIST Federal Computer Security Standards:** Contractors must comply with all applicable HIPAA Security Rule Standards as well as the most current version of *NIST Special Publication 800-53 Federal Computer Security Standards and Controls* that are applicable to the information system. Security controls shall be implemented to comply with a Data Security Categorization Risk Level of "*Moderate*" as defined by the NIST/FIPS 199 Standard.

R5. **NIST/FIPS 197, Advanced Encryption Standard:** Contractor's solution shall comply with the requirements of this standard where applicable or shall utilize other NIST/FIPS-approved encryption protocols and cryptographic algorithms where appropriate.

R6. **NIST/FIPS 140-3, Security Requirements for Cryptographic Modules:** Contractor's solution must meet the requirements of this standard at Level 2 or Higher. This standard addresses the use of approved security functions in computer cryptographic services such as cryptographic algorithms, cryptographic key management techniques, authentication techniques and digital signatures that have been approved for protecting sensitive Federally regulated information. This standard covers cryptographic module implementations including but is not limited to, hardware components or modules, software/firmware programs or modules or any combination thereof.

R7. **NIST Special Publication 800-88, Guidelines for Media Sanitization:** Contractors solution and services must comply with the requirements of this standard. The media sanitization method utilized for all media containing State data shall be based on a NIST/FIPS 199 data security categorization risk level of "Moderate" risk. This includes data stored on all computing devices, storage devices and media types.

R8. **Social Security Administration (SSA) Technical System Security Requirements:** Prior to being allowed access to SSA-derived data, the contractor's solution must meet the most current version of SSA Technical System Security Requirements (TSSR). Contractor agrees to document and provide a completed and approved SSA Security Evaluation Questionnaire (SEQ) and ensure that their solution meets SSA Certification Standards as detailed in the TSSR.

R9. State Enterprise Information Security Policies and Standards: Contractor's solution and services shall comply with applicable State of Georgia Enterprise Information Security Policies and Standards where applicable, unless an exception is approved in writing by DCH. If a standard or requirement conflict exists with GTA State Standards, Agency Computer Security Policies and Standards shall be followed.

R10. Georgia Department of Community Health Security Standards: Contractor must comply with applicable DCH Information Security Policies and Security Control Configuration Standards, where applicable.

R11. DCH Password Security Standards: Contractor's solution must meet DCH State Agency Password Security Standards for length, complexity, aging, and reuse to meet the following:

1) Length – Passwords must be a minimum length of at least eight characters.
2) Complexity – Passwords must contain both uppercase and lowercase letters and at least one non-alphabetic character, and to not be a "dictionary" word.
3) Aging – All Passwords must expire every 45 days.
4) Reuse – Passwords must not be reused.

R12. DCH E-Mail, Mobile Device and Data Storage Encryption Security Standards: Contractor's solution shall ensure that all sensitive and confidential State data is encrypted during transmission as well as, while at rest or where stored (i.e. data that resides in e-mail, databases, file systems, server and cloud based platforms, fixed or removable production/back-up media, wireless and mobile devices or other structured storage methods. This includes data which resides in both production and disaster recovery platforms. Encryption solutions must meet the most current versions of NIST/FIPS Encryption and Cryptographic Standards. Full-Disk Encryption solutions shall be utilized where applicable (i.e. wireless and mobile devices, san storage units, fixed or removable media such as computer servers, hard drives, flash drives, etc.)

R13. Information System Security Plans: Prior to being allowed access to State data**,** contractor must provide to the State with a detailed Information System Security Plan (SSP) which details how their system/application solutions and services meet applicable NIST Special Publication 800-53 Moderate-Impact-Baseline Federal Computer Security Controls/Sub-controls and Requirements. The SSP must address all criteria contained within the NIST Special Publication 800-18 System Security Plan Template. The SSP should address all applicable Infrastructure, Network, System, and Application Security Controls which are in scope for the contracted services and address controls/sub-controls outsourced to subcontractors and third-party service providers (including CSP's). The system security plan must be submitted to the DCH cybersecurity office for review and approval. All non-compliant SSP control implementation descriptions must be corrected prior to SSP approval. The SSP must be reviewed and updated by the contractor at least, annually or at such time as major system or architecture changes occur to the contractor's solution.

R14. **Disaster Recovery Plans/Annual DR Exercise Reports:** Contractor must maintain current and fully operational Disaster Recovery and Business Continuity Plans in order to provide immediate response and subsequent recovery of State data from any unplanned service interruptions. These Plans shall be updated and exercised at least annually. Service Provider shall ensure that the appropriate security and privacy controls are in place for the protection of sensitive and confidential State data on the DR Platform. This includes the encryption of transmitted and stored State data. Contractor shall provide DCH with a documented copy of their Disaster Recovery Plans and Annual DR Exercise Reports for review and approval.

R15. **Offshore Data Use:** Contractor must ensure that State data is not used, maintained, transmitted, stored, accessed or processed in geographic or virtual areas which are not subject to U.S. Law.

R16. **Cloud Infrastructure Protections:** Contractor solutions utilizing virtualized cloud computing platforms to deliver services to the State and store sensitive and confidential data shall ensur6e that these environments comply with the appropriate NIST security controls and Infrastructure protection measures in order to prevent the loss or unauthorized access, destruction, use, modification or disclosure of State data. These safeguards shall include the following: FedRAMP Certified Government or Commercial Cloud Infrastructure Platform, Data Segregation, Logical Service/Host Separation, Network Intrusion Detection and Prevention, Firewalls, Virus/Malware Protections, appropriate Security Updates and Patching of Virtual Machine Images, etc. CSP services utilized must employ security controls that meet NIST 800-53 Moderate Impact Baseline Security Control Standards.

R17. **Data Segregation:** Contractor solutions consisting of physical or virtualized cloud computing platforms shall ensure that the Systems, Applications, and Data used to provide State services are physically and/or logically segregated from third-party Systems and Data.

R18. **Multi-Factor Authentication (MFA):** Contractor solutions must employ Multi-factor Authentication digital identity guideline access control solutions for All Users with access to State Data except, for Public Facing User Accounts which do not have logical access to State Data. MFA technology solutions employed must meet the NIST Special Publication 800-63B Digital Identity Guidelines Standards at an Authenticator Assurance Level 2 (AAL2) or Higher Standard.

R19. Security Alerts. Contractor systems and software application solutions shall alert the appropriate authorities and staff of potential violations of security policies, controls and safeguards such as, the inappropriate access to sensitive and confidential information. Contractor's solution shall contain mechanisms to monitor transaction based events and support the appropriate activity logging.

R20. Security Incident Response: Contractor shall employ formal, structured and documented organizational policies and procedures to detect and respond to Cybersecurity Incidents. IRP Procedures shall employ methodologies and guidelines detailed in the most current version of NIST Special Publication 800-61, Computer Security Incident Handling Guide. For security and privacy incidents which may involve Personally Identifiable Information, SSA-derived Data or Protected Health Information, DCH Policy 915 Privacy & Security HIPAA Incident Response Policies and Procedures must be followed.

R21. Infrastructure Protection Measures: Contractor solutions shall implement the appropriate infrastructure protection measures in order to protect State data. This includes Network/Host Intrusion Detection and Prevention, Firewalls, Proxies, Anti-Malware Detection and Prevention, Security Patches, Web Content Filters, E-Mail Transmission Encryption, etc.

R22. Formal Change Management Process: Contractor shall ensure that all service affecting production system or software application changes follow a formal documented change management process which includes a security risk analysis.

R23. Boundary Protection Measures: Contractor shall ensure that the appropriate system boundary protection controls and measures are in place for the protection and monitoring (i.e. active monitoring) of the systems and software applications hosting State data against malicious program code, denial of service attacks, network and system intrusions, and other cyber-attacks. Systems shall alert the appropriate parties responsible for monitoring and responding when these suspicious conditions exist.

R24. Role Based Access Control: Contractor solutions shall support identity and access management functionality including the "separation of duties", the "principal of least privilege", and "role based access controls" as well as, a user security profile that controls access rights to data categories and system functions.

R25. Default System Accounts: Contractor shall ensure that all unnecessary default system and application login accounts are removed or disabled within the solution platform.

R26. Transmission Integrity Controls: Contractor shall ensure that systems and applications hosting State data support data integrity controls to guarantee that transmitted information is not improperly modified without detection (e.g. provide for secure data transmission).

R27. Annual Third-Party Security Assessments: Contractor shall conduct an Annual Independent Third-Party NIST SP 800-53 Controls/Sub-controls based security assessment of the service delivery platform. Control criteria must be based on NIST Moderate-Impact-Baseline Controls. Contractor shall provide the State with an Annual Security Assessment Report (SAR) which contains a detailed control gap analysis. All identified security control non-compliance gaps identified must be detailed in and a Plan of Action and Milestones (POA&M) Report which specifies a gap remediation plan and expected remediation dates for any identified security control gaps or assessment findings. Independent Security Assessment Reports and POAM Reports must be submitted to the State annually for review and approval. Contractor shall make regular reports to the State in writing regarding the current remediation status of the security control gaps. Each POAM Item shall be categorized by severity level (High, Moderate and Low) based on NIST Risk Management Framework Guidelines.

R28. Non-repudiation: Contractor solutions and platforms shall support non-repudiation methodologies in order to ensure that transmission services provide proof of the integrity and origin of sensitive and confidential data. Solution shall employ authentication services which can be asserted to be genuine with high assurance (e.g. use of NIST approved cryptographic controls and digital certificates).

R29. Personnel Background Security Screening: Contractor and its subcontracted staff as well as, its third-party service organizations shall verify the identity, employment eligibility, and must conduct background security screenings for all employees, contractors, suppliers, third-parties and others, prior to allowing their access to State data. Contractor shall address this requirement in all third-party service agreements used to deliver services to the State.

R30. Secure Interfaces: Contractor must ensure that all connections to its information systems or software applications used to deliver services to the State which originate from outside the security boundary of the systems or applications, shall be fully documented, authorized, and occur only through secure controlled interfaces (e.g. Proxies, Gateways, Routers, Firewalls, Encrypted Tunnels, etc.) and be continuously monitored.

R31. Security Event & Activity Log Monitoring: Contractor solutions used to provide State services shall support security event, transaction and activity log monitoring mechanisms to prevent the loss or unauthorized access, destruction, use, modification or disclosure of State data. Log data shall be routinely reviewed and analyzed by the appropriate trained personnel. Logging systems, configurations and files shall be protected from breaches of confidentiality and integrity. Access to logs files and log configurations/generators shall be audited, monitored and restricted to need-to-know personnel. Log events shall include the following, at a minimum:

- User IDs
- Dates and times of account logon/logoff
- Logon method, location, terminal identity (if possible), Network address
- Unsuccessful system or data access attempts
- All actions performed using privileged access
- System alerts or failures

R32. Digital Identity Guidelines: Contractor's solution must meet or exceed the guidelines specified in the most current version of NIST SP 800-63B, Digital Identity Guidelines. All User identity and Access Management solutions employed must meet NIST Identity Access Management Assurance Level 2 (IAM2) as well as, Authenticator Assurance Level 2 (AAL2) Standards.

R33. MEST SI Integration Platform Support: Contractor shall collaborate with the State and its Systems Integration Services Supplier to integrate the Contractor's solution into the State's system integration platform including the implementation of single sign-on (SSO), MFA and federated identity management integration solutions.

R34. Vulnerability Management Program Plan: Contractor will provide supporting documentation to the State which demonstrates that a Formal Vulnerability Management Plan, Processes, Procedures have been implemented which addresses continuous security monitoring of the contractor's networks, system(s) and software applications used to provide services to the State. This should include Network, System and Application and Infrastructure Vulnerability Scanning and Penetration Testing Activities per NIST CSF and CRR Frameworks.

R35. Data De-identification and Data Re-identification: Contractor's solution shall have the capability to de-identify and/or redact sensitive and confidential data for entities not authorized to view, access or receive PII, PHI and SSA-derived Data. The solution must utilize de-identification algorithms to allow for re-identification of data, if required.

R36. Production/Non-Production Data Redaction: Contractor shall provide a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data (e.g., PII/PHI, SSA-derived Data, etc.) when extracting data from the production environment for use in non-production environments.

R37. Organizationally Defined NIST Federal Security Control Configuration Settings: Contractor shall request guidance from the State concerning the specific Agency configuration setting, thresholds and standards to be met pertaining to the implementation of applicable NIST Federal Computer Security Controls/Sub-controls which may require organizationally defined parameters.