SECURITY STANDARDS FOR THIRD PARTIES

The following standards must be followed by any third-party in order to host DOM data, systems, or applications:

Category	Standard Description
Policy and Procedures	Provider must comply with NIST Standards.
	Provider must comply with HIPAA and HITECH regulations.
	Provider will be responsible for HIPAA training for all staff – subject to review and approval by the Division of Medicaid.
	Provider must complete all requested security compliance documents regarding IT infrastructure and services.
	Provider staff will undergo a full background check with all findings reported to DOM at the execution of the initial contract. Any new provider staff must also undergo a full background check and supplied to DOM.
	Provider must supply DOM with a complete list of services or vendors related to DOM data to ensure security. This list must be continually updated and also include contact information.
Administrative Safeguards	Contact Two Factor authentication that meets FIPS 140-2 Level 4 for all employees.
	Provider is responsible for all fines and penalties of breach of security or HIPAA violation.
	DR/BCP updated quarterly, tested annually with all deficiencies documented and with a remediation plan presented to DOM at conclusion of tests. DOM recommends that the DR site be operational within 48 hours after DOM declares a disaster or at a time dictated by contract.
	Gap analysis, penetration test, and a vulnerability assessment will occur every other year. However, the vulnerability assessment will be performed annually, and all data will be shared with DOM. A copy without redaction may be required.
	All technicians/supervisors/managers/directors will be certified on systems they administer and renew certifications as required by manufacturer/vendor. SMEs must be certified at the most current certification path.
	Network monitoring systems will be utilized (IDS, IPS, AV, Log Manager) and data will be retained for a minimum of 24 months. Additionally, ASA, VPN, Firewalls, Authentication mechanisms shall be utilized and require network monitoring for intrusion detection. All reports should be rendered in a readable format.
	The maximum downtime for any system/application failure will be 4 hours.
	Provider must have well established SLAs that meet the requirements of DOM, the Fiscal Agent, and third party contract requirements. There must also be proactive credits for SLA violations.
Physical Safeguards	Physical access control to all facilities/racks that have access to the hosted DOM data that meets or exceeds FIP 201-2. Free egress is not allowed, so all staff must badge in and out individually.
	Service personnel and visitors will be escorted and accompanied by a data center employee at all times. Additionally, tours of the data center clients should be limited to individual/clients only for business purposes.
	Provider must have a security incident process that allows for 24/7 access with appropriate levels of support personnel available if the primary is un-available.

Category	Standard Description
	If the provider is housing DOM owned equipment, then the provider must have 24/7/365 video surveillance to facility and racks that hold, transmit, or have access to DOM data. Additionally, the data center must maintain 24 months of video that can be replayed/downloaded on demand by DOM with access to real time video.
	Provider must provide 24/7 technical support when needed. Tier 3 level engineer support must be available when a call is placed to the Operations Center.
	Provider must have 24/7/365 Security.
	Access to the data center will require the following three conditions: 1) Biometric hand scanner, 2) Card access, and 3) Pin number.
	All racks must employ the highest level of security as technology allows.
	Facility must be SAS 70 compliant and have a SOC 2 Report available.
Technical Safeguards	All data will be secured in the highest manner possible. All data at rest will be encrypted, and data in flight will be encrypted as technology allows.
	Data will not be co-mingled with any other data and will be segregated from any other network traffic and data.
	Provider must ensure that all environments (Development, QA, Test, etc) are maintained and do not impact the Production environment.
	A list of open ports will be provided to DOM for review. In order to maintain appropriate security integrity, the provider must ensure that all ports not identified to maintain operations will be blocked by default.
	DOM prefers fully redundant virtual environments with high availability enabled.
	The provider must have continuous operation during power failure.
	Provider must ensure a certain level of quality and assurance to prevent degradation in services or conflicts in the virtual environment by other virtual services.