The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to policies, procedures and documentation requirements, and the appointment of a security official.

The Department shall adopt and follow the State HIPAA policies and procedures.

The Commissioner of the Department and her/his designees, along with the ITSU, are responsible for establishing, implementing, and enforcing State HIPAA Security policies and procedures.

State HIPAA Security policies and procedures do not preempt any existing or similar laws or policies.

The State HIPAA policies and procedures apply to all ePHI and IT resources that store, process, have access to, and/or transmit ePHI held by the covered entities and covered components of hybrid entities.

Policies and procedures shall be reasonable and appropriate to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, taking into account:

- the size, complexity, and capabilities of the Agency
- the Agency's technical infrastructure, hardware, and software capabilities
- the costs of security measures, and
- the probability and criticality of potential risks to ePHI.

Centralized procedures shall be developed by the ITSU for those procedures that are to be used by all agencies. Agencies shall develop decentralized procedures that must be specific to their state agency to define specific operational steps for policy compliance.

Guidelines that set forth “best practices” shall be developed by the ITSU for the purpose of assisting agencies to comply with policies and procedures.

Policies, procedures, and guidelines shall be documented and stored by the agencies and the ITSU, in paper form or electronically.

HIPAA Security Rule's policies, procedures and actions, activities or assessments, required by the HIPAA Security Rule, including by not limited to, risk analysis, evaluations, and documentation related to security incidents and their outcomes, shall be maintained for six years from the creation date or the date when it last was in effect, whichever is later.

- Documentation shall be made available to anyone responsible for implementing, managing, and auditing the procedures to which the documentation pertains. Documentation shall be reviewed, updated and modified, as needed, if environmental or operational changes affect the security of ePHI.
The Department shall identify a security official who will be responsible, in conjunction with the ITSU, for the development and implementation of the policies and procedures required for compliance with the HIPAA Security Rule.

The following policies shall be adopted and enforced as applicable:

- HIPAA Administrative Policy
- Security Awareness and Training Policy
- Acceptable Use and Sanction Policy
- Information Technology Access Policy
- Information Technology Security Policy
- Information Technology Activity Review and Logging Policy
- Incident Response and Reporting Policy
- Information Technology Resource Management Policy
- Facility Security Policy
- Business Continuity Planning & IT Disaster Recovery Policy
- Risk Management and Audit Policy