HIPAA Security Standards: Summary

ADMINISTRATIVE SAFEGUARDS:

1.  Security Management
   a.  Risk analysis (**REQUIRED**) – Conduct a security risk assessment for systems utilizing e PHI.
   b.  Risk Management (**REQUIRED**) – Document risk assessment findings and develop a plan to fix deficiencies in security.
   c.  Sanction policy (**REQUIRED**) – Develop a policy describing the sanctions imposed when persons violate University policy.
   d.  Information System activity review (**REQUIRED**) – Develop and document procedures to monitor system activity audit logs, and regularly review user access reports, and security incident records.

2.  Assigned security responsibility (**REQUIRED**) – Designate an individual who is responsible for the security program.

3.  Workforce Security
   a.  Authorization and/or supervision (**ADDRESSABLE**) – Develop process and procedure to supervise and/or monitor for unauthorized staff activity.
   b.  Workforce clearance procedures (**ADDRESSABLE**) – Regularly review user access authorizations for applicability, and perform background checks on new staff.
   c.  Termination procedures (**ADDRESSABLE**) – Develop procedures to ensure prompt removal of access rights for terminated staff.

4.  Information Access management
   a.  Isolate health care clearinghouse functions (**REQUIRED**) – Not applicable.
   b.  Access authorization (**ADDRESSABLE**) - Document procedures for granting appropriate access to users.
   c.  Access establishment and modification (**ADDRESSABLE**) – Document procedures to review, change access of authorized users as needed.

5.  Security awareness and training
   a.  Security reminders (**ADDRESSABLE**) – Provide periodic reminders about security to users.
   b.  Protection from malicious software (**ADDRESSABLE**) – Provide antivirus software to protect assets against malicious software.
   c.  Login monitoring (**ADDRESSABLE**) – Implement a method to monitor login activity to protected systems.
   d.  Password management (**ADDRESSABLE**) – Implement policy and procedure to ensure strong password rules are followed.

6.  Security incident procedures

7.  Contingency Plan
   a.  Data backup plan (**REQUIRED**) – Develop and document process and procedures for data backup and recovery.
   b.  Disaster Recovery plan (**REQUIRED**) – Develop a disaster recovery plan.
   c.  Emergency mode operation plan (**REQUIRED**) – Document alternative (manual?) procedures for operating in the event of an emergency such as a system outage.
   d.  Testing and revision procedures (**ADDRESSABLE**) – Document the process for review and testing of contingency plans.
   e.  Applications and data criticality analysis (**ADDRESSABLE**) - Perform an assessment of applications and data to determine classification and criticality.

8.  Evaluation (**REQUIRED**) – The whole security plan and supporting documentation must be evaluated on a periodic basis.
HIPAA Security Standards: Summary

PHYSICAL SAFEGUARDS:

1. Facility Access Controls
   a. Contingency operations (ADDRESSABLE) – Document procedures for allowing facility access in emergency situations.
   b. Facility Security plan (ADDRESSABLE) – Document policies and procedures to safeguard the facility and equipment.
   c. Access control and validation procedures (ADDRESSABLE) – Document the process for authorizing, implementing, and regularly reviewing physical access to facilities which house computer systems.
   d. Maintenance records (ADDRESSABLE) – Document all system and facility security maintenance activities.

2. Workstation Use (REQUIRED) – Document policy and procedure regarding the acceptable use of workstations, including authorized functions for locations.

3. Workstation Security (REQUIRED) – Physical safeguards to protect workstations used to access e-PHI.

4. Device and Media Controls
   b. Media Re-Use (REQUIRED) – Procedures for removal of e-PHI from media before its reuse.
   c. Accountability (ADDRESSABLE) – Maintain records of hardware & media movement.
   d. Data backup and storage (ADDRESSABLE) - Create an image copy of e-PHI before any movement of equipment.

TECHNICAL SAFEGUARDS:

1. Access Control
   a. Unique user identification (REQUIRED) – Each user must be individually identifiable.
   b. Emergency access procedure (REQUIRED) – Document procedures for providing emergency access authorization to systems.
   c. Automatic logoff (ADDRESSABLE) – Force an automatic logoff from systems after a certain amount of inactivity.
   d. Encryption and decryption (ADDRESSABLE) – Implement a mechanism to encrypt and decrypt e-PHI.

2. Audit controls (REQUIRED) – Implement mechanisms to record and examine activity on systems with e-PHI.

3. Integrity
   a. Mechanism to authenticate e-PHI (ADDRESSABLE) – Implement controls to ensure e-PHI has not been altered or destroyed in an unauthorized manner.

4. Person or entity authentication (REQUIRED) – Implement procedures to verify identity before allowing access to e-PHI.

5. Transmission security
   a. Integrity controls (ADDRESSABLE) – Implement security measures to ensure e-PHI is not improperly altered without detection.
   b. Encryption (ADDRESSABLE) – Implement measures to encrypt e-PHI when appropriate.

ORGANIZATIONAL REQUIREMENTS:

1. Business Associate Contracts or other arrangements, includes subcontractors.
   a. Business Associate contracts (REQUIRED) – Draw up contracts to ensure business associates will implement adequate protections for e-PHI, and will report security incidents to the covered entity.
   b. Other arrangements (REQUIRED) – Similar arrangements for government agencies.
HIPAA Security Standards: Summary

2. Requirements for group health plans (REQUIRED) – Amend group plan documents to ensure adequate protections for e-PHI are implemented, and security incidents are reported.

Policies, Procedures, and Documentation Requirements:

1. Policies and Procedures (REQUIRED) – Implement reasonable and appropriate policy and procedures to comply with the standards.
2. Documentation
   a. Time Limit (REQUIRED) – Maintain documentation for 6 years.
   b. Availability (REQUIRED) – Make documentation available to all affected people.
   c. Updates (REQUIRED) – Review and update all documentation periodically.