

## Brief Summary of Key Points of HIPAA Security For PHS Research

2/8/2005

Similar to the HIPAA Privacy Standards, The HIPAA Security Standards are concerned with Protected Health Information (PHI), but they are specifically aimed at ways to protect electronic PHI (ePHI), either at rest or in transmission, and don't cover paper based PHI.

The standards for protecting ePHI are divided into categories of Administrative, Physical, and Technical, and each standard has an implementation specification which is either "Required"(R) or "Addressable"(A). Addressable specifications allow for a more flexible response.

### **Administrative:**

- Each site must inventory their systems (hardware/software), determine the priority/criticality, the security risks present, and take steps to address them (R)
- As in Privacy, there must a sanctions policy for non compliance with standards (R)
- System audits, manual or automated, must occur regularly (R)
- There must be a designated Security Officer responsible for the standards (R)
- Authorization/supervision should exist to guarantee the correct, and only the correct persons have access to the PHI data as needed – this includes supervision of environmental and facilities personnel who may have physical access. (A)
- All personnel with access should be cleared through CORI checks, or equivalent (A)
- A Transfer Policy and a Termination Policy that removes or changes passwords, keys and other access should exist and be audited (A)
- There should be a procedure for granting proper access, through passwords, program control, etc. "Strong" passwords, or equivalent should be required; "Role based access" should be present where meaningful, and access must be managed and audited, including logon monitoring. (A)
- There should be a Security Awareness Program, for initial training and for timely updates. (A)
- There should be procedures for protection against Viruses, Worms, and other malicious software. (A)
- Security incidents must be recorded and formally reported with associated responses (R)
- Contingency plans must exist, and be regularly tested, for short term and long term outages or crises. Regular system backups are included, as well as procedures for restoration. (R)
- The initial security assessment process must be repeated regularly to address changes and improve status. (R)
- As in Privacy, Business Associate Contracts are necessary if data is shared outside the organization; they must be modified to address the security issues detailed here. (R)

**Physical:**

- Emergency contingency plans should include facility access procedures (A)
- A regularly maintained facility security plan with access control procedures should exist (A)
- There should be a policy to control and document maintenance of computer systems, facility locks, and network wiring area (A)
- There must be use policies for Workstations/PC's/Portables that provide proper data security and also protection from malicious software, at work or in the home (R)
- A procedure for proper disposal of data and systems that contain data must exist, as well as a procedure for reuse of media (R)
- Movement of systems (hardware and/or software) should be recorded (A)
- A data backup system should exist (A)

**Technical:**

- Each user of a system must be identifiable (no shared logons) (R)
- There must be a procedure for emergency access to a system in the absence of a system manager (R)
- Automatic logoff should exist on each system (A)
- Approved data encryption techniques should be available, and a policy should define its use (A)
- Audit controls, automatic (logs) and/or manual, must exist for each system, and documented procedures should determine their frequency of use (R)
- Integrity of data should be guaranteed through automated means (e.g. checksum) or manual quality reviews. (A)
- User authentication must exist on each system: Unique Logons with “Strong” passwords, and “Role based access” should be present where meaningful, and access must be managed and audited, including logon auditing. (R)
- Data transmission networks should be protected against unauthorized access. (A)

**Policies, Procedures & Documentation Requirements:**

- Policies and procedures must be reviewed and updated regularly (R)
- Documentation must be retained for 6 years from the date of its creation or the date when it last was in effect, whichever is later (R)