

# SECURITY REGULATION OUTLINE PROPOSED

(This regulation is not yet finalized.)

*The following HIPAA regulation outline must only be used as a high-level reference guide and not as a warranty or representation of Misys Healthcare Systems. You should obtain copies of the HIPAA final and proposed regulations in their entirety for complete details and descriptions.*

*The Department of Health and Human Services (HHS), the agency responsible for creating rules and regulations to comply with HIPAA, maintains a web site. This web site provides links to the Final and Proposed rules along with Frequently Asked Questions, Press Releases, Milestones, etc. relating only to Administrative Simplification. The HHS web site address is:*

*[www.aspe.hhs.gov/admsimp](http://www.aspe.hhs.gov/admsimp)*

**The HIPAA Security Regulations propose standards for the physical protection of individual health information. The electronic signature portion of the regulation has been removed and could be in a separate/future proposed standard. Below is an outline of the proposed security regulation.**

## **Administrative Procedures**

Guard Data Integrity, Confidentiality and Availability  
(Proposed Security)

- **Certification** - Evaluation of computer system or network design to certify that the appropriate security has been implemented. Evaluation could be performed internally or by an external accrediting agency.
- **Chain of Trust Partner Agreement** This is a contract in which parties agree to electronically exchange data and to protect the transmitted data. This ensures the same level of security is maintained when information moves from one organization to another.
- **Contingency Plan** - Policies and procedures for system emergencies. (Five required implementation features).
  - Application and data criticality analysis.
  - Data backup plan.
  - Disaster recovery plan.
  - Emergency mode operation plan.
  - Testing and revision.

- **Formal Mechanism for Processing Records** - Documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and or disposal of health information. This is important to limit the inadvertent loss or disclosure of secure information because of process issues.
- **Information Access Control** - Requirement to establish and maintain formal, documented policies and procedures for granting different levels of access to health care information. (Three required implementation features).
  - Access authorization.
  - Access establishment.
  - Access modificaiton.
- **Internal Audit** - To enable the organization to identify potential security violations, an ongoing internal audit process would be required, i.e., an in house review of the records of system activity including logins, file accesses, and security incidents must be maintained by the entity.
- **Personnel Security** - To prevent unnecessary or inadvertent access to secure information. All personnel with access to health information must be authorized to access health information after receiving appropriate clearances. (Six required implementation features)
  - Assure supervision of technical maintenance personnel by authorized, knowledgeable person.
  - Maintenance of record of access authorizations.
  - Operating, and in some cases, maintenance personnel have proper access authorization.
  - Personnel clearance procedure.
  - Personnel security policy/procedure.
  - System users, including technical maintenance personnel, trained in security.
- **Security Configuration Management** - Implementation of measures, practices and procedures. This would be coordinated and integrated with other system configuration management practices to manage system integrity. This integration would ensure that routine changes to system hardware or software do not contribute or create security weakness. (Five required implementation features)
  - Documentation
  - Hardware/software installation & maintenance review and testing for security features.
  - Inventory
  - Security Testing.
  - Virus checking.

- **Security Incident Procedures** - To ensure that security violations are reported and handled promptly. Organizations would be required to implement accurate and current security incident procedures. (Two required implementation features)
  - Report procedures.
  - Response procedures.
  
- **Security Management Process** - To ensure the prevention, detection, containment and correction of security breaches, a process for security management is required. Requirements include the establishment of accountability, management controls (policies and education), electronic controls, physical security and penalties for the abuse and misuse of its assets (both physical and electronic). (Four required implementation features)
  - Risk analysis.
  - Risk management.
  - Sanction policy.
  - Security policy.
  
- **Termination Procedures** - Policies and procedures (Four required implementation features).
  - Combination locks changed.
  - Removal from access lists.
  - Removal of user account(s).
  - Turn in keys, token or cards that allow access.
  
- **Training** - Policies and procedures (Five required implementation features).
  - Awareness training for all personnel (including management).
  - Periodic security reminders.
  - User education concerning virus protection.
  - User education in importance of monitoring log in success/failure, and how to report discrepancies.
  - User education in password management.

## **Physical Safeguards**

Guard Data Integrity, Confidentiality and Availability  
(Proposed Security)

- **Assigned Security Responsibility** - Assigned and documented individual or organization responsible for the management and supervision of security measures and conduct of personnel in relation to protected data.
- **Media Control** - Policies and procedures that govern the receipt and removal of protected health information in and out of the facility (example diskettes, tapes). (Five required implementation features)
  - Access control.
  - Accountability (tracking mechanism).
  - Data backup.
  - Data storage.
  - Disposal.
- **Physical Access Control** - Formal documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. (Nine required implementation features)
  - Disaster recovery.
  - Emergency mode operation.
  - Equipment control (into and out of site).
  - Facility security plan.
  - Procedures for verifying access authorizations prior to physical access.
  - Maintenance records.
  - Need-to-know procedures for personnel access.
  - Sign-in for visitors and escort, if appropriate.
  - Testing and revision.
- **Policy / Guideline on Workstation Use** - Policies and Procedures (example logging off before leaving a terminal unattended).
- **Secure Workstation Location** - Physical safeguards.
- **Security Awareness Training** - Security awareness training for all employees based on job responsibilities.

## **Technical Security**

Guard Data Integrity, Confidentiality and Availability  
(Proposed Security)

- **Access Control** - Requirement for restricting access to resources and allow access only by privileged entities. Emergency access is required and must be documented. In addition, at least one of the following features must be implemented: Context, Role or User based access. Encryption is optional. (Two required implementation features.)
  - Procedure for emergency access
  - Context, Role or User based access (one is required)
- **Audit Controls** - Requirement for control mechanisms to record and examine system activity. These mechanisms would identify suspect data access activities, assess its security program and respond to potential weaknesses.
- **Authorization Control** - Only properly authorized individuals will have access to protected health information for use and disclosure. Either Role or User based access must be implemented. (Two options; one required implementation feature)
  - Role or User based access. (one is required)
- **Data Authentication** - Requirement to be able to provide corroboration that data in possession has not been altered or destroyed in an unauthorized manner. Examples to assure data corroboration include check sum, double keying, message authentication code or digital signature.
- **Entity Authentication** - Requirement to corroborate that an entity is who it claims to be. Authentication would be important to prevent improper identification of an entity who is accessing secure data. The following implementation features would be used: automatic log off and unique user identification. In addition one of five required implementation features would be used. (Three required implementation features.)
  - Automatic logoff.
  - Unique user identification
  - Biometric, Password, PIN, Telephone call back, or Token (one is required).

## **Technical Security Mechanisms**

Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network

### **(Proposed Security)**

Each organization that uses communications or networks would be required to protect communications containing health information that are transmitted electronically over open networks so they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access their systems through external communication points. When using open networks, some form of encryption should be employed. **The utilization of less open systems / networks such as those provided by a value-added network (VAN) or private-wire arrangement provides sufficient access control to allow encryption to be an optional feature.** These controls are important because of the potential for compromise of information over open systems such as the Internet or dial-in lines.

The following implementation features would be in place:

- Integrity controls
- Message authentication

One of the following implementation features is required:

- Access controls
- Encryption

In addition, if using a network for communications, the following implementation features are required:

- Alarm
- Audit Trail
- Entity Authentication
- Event Reporting

## **Electronic Signature** **(Proposed Security)**

1. Digital Signature - If electronic signatures are employed, digital signature technology is required. **Currently no HIPAA Transaction Standard requires Electronic Signature (page 43246)**. If electronic signatures are used, certain implementation features must be included, specifically:
  - Message integrity
  - Nonrepudiation
  - User authentication
  - Additional / other implementation features are optional.