DILEY RIDGE MEDICAL CENTER

HIPAA Information Security Overview

Revised 1/2011

Security Overview

HIPAA Security Regulations establish safeguards for protected health information (PHI) in electronic format. The security rules apply to PHI that is electronically transmitted from one location to another as well as PHI that may be used or stored by Diley Ridge Medical Center. The rules were developed based on current computer industry standards and best practices. The deadline to comply with the security regulations was April 21, 2005.

The Security Rule does not address the extent to which an entity should implement the specific features and requires that each entity assess its own security needs based on risk assessment. An organization is responsible for their choice of technology, as well as for meeting individual security requirements. As part of HIPAA compliance, Diley Ridge Medical Center developed security policies and procedures to ensure confidentiality, integrity and availability of electronic protected health information (PHI).

Information Security Officer

HIPAA requires that organizations create the role of Security Officer. The Security Officer's primary responsibility is to oversee an organization's compliance with HIPAA security regulations. He or she ensures that the organization implements appropriate information security policies and procedures, performs risk analysis, responds to employee questions and concerns, and resolves information security related issues. At Diley Ridge Medical Center, the Information Security Officer is Tom Enneking who can be reached at 614-898-8708 or via e-mail at tenneking@mchs.com.

Information Security

The security rules define three key parts for information security. These include the following:

- Administrative safeguards- administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI.
- Physical safeguards- physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards including unauthorized intrusion.
- Technical safeguards- the technology and policy and procedures for its use that protect electronic PHI and control access to it.

Together, these requirements define the basic level of security that must be in place in order to comply with HIPAA.

Administrative Safeguards

Under the security rules, written policies, procedures and processes must be in place. The primary purpose of Administrative Safeguards is to identify how to protect information from improper access, use and disclosure.

Administrative Safeguards include the following nine standards:

1. **Security Management Process**
   - Risk Analysis: A process where cost effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.
   - Risk Management: A process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.
   - Sanction Policies: Statements regarding disciplinary actions that are communicated to all employees, agents and contractors.
   - Information System Activity Review: Records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. **Assigned Security Responsibility**
   - Identify the security official who is responsible for development and implementation of security policies and procedures.

3. **Workforce Security**
   - Authorization and/or supervision: Procedures for the authorization and /or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.
   - Workforce Clearance: Procedures to determine the access of a workforce member to electronic PHI is appropriate.
   - Termination: Procedures for terminating access to electronic PHI as required.

4. **Information Access Management**
   - Implement policies and procedures for authorizing access to electronic protected health information.
   - Review and modify a user's right of access to a workstation, transaction, program or process.

5. **Security Awareness and Training**
   - Security reminders: Periodic security updates.
   - Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.
   - Log-in monitoring: Evaluate log-in attempts and reporting discrepancies.

- Password management: Procedures for creating, changing, and safeguarding passwords.

6. **Security Incident Procedures**
   - Response and reporting: Procedures to handle any incident that results in a security breach. All violations of the security standards must be reviewed and handled as quickly as possible. Corrective actions should also take place to eliminate or to reduce the potential for further violations.

7. **Contingency Plans**
   - Data back-up plan: Create and maintain retrievable copies of electronic PHI.
   - Disaster recovery plan: Establish and implement procedures to restore any loss of data.
   - Emergency mode operation plan: Establish and implement procedures to enable continuation of critical business functions for protection of the security of electronic PHI while operating in emergency mode.
   - Testing and revision procedures: Periodic testing of and revision of contingency plans.
   - Applications and data criticality analysis: Assess the relative criticality of specific applications and data in the support of contingency plan.

8. **Evaluation**
   - Perform a periodical evaluation of in response to the environmental or operational changes affecting the security of electronic PHI.

9. **Business Associate Contracts**
   - Written contract or other arrangement: Diley Ridge Medical Center may permit a business associate to create, receive, maintain, or transmit electronic PHI on Diley Ridge Medical Center's behalf if satisfactory assurances that the business associate will appropriately safeguard the information.

Physical Safeguards

The purpose of the physical security measures is to help protect the physical computer system, building and equipment from the following:

- Fire
- Other natural and environmental hazards
- Unauthorized access

These measures include locks, keys, badges or cards that unlock doors and other steps to restrict access to computer systems and facilities (e.g. passwords). Physical security also includes administrative processes such as written policies and procedures.

Physical Safeguards include the following four standards:

1. **Facility Access Controls**
   - Contingency operations: Procedures to that allow facility access in support of restoration of lost data in the event of an emergency.
   - Facility security plan: Procedures implemented to safeguard the facility and equipment unauthorized access, tampering, and theft.
   - Access control and validation procedures: Control and validation of access to facilities based on role including visitor control, and control of access to software programs for testing and revision.

2. **Workstation Use**
   - Implementation of policies and procedures that specify the proper functions to be performed and the physical attributes of the surroundings of workstations that can access electronic PHI.

3. **Workstation Security**
   - Workstations, computer systems, and printers need to be secured from unauthorized viewing or use. Where and how equipment is placed can affect security. If the employee or physician leaves the computer, he or she should log out of the system.

4. **Device and Media Controls**
   - Disposal: Procedures to address the final disposition of electronic PHI and the hardware or electronic media on which it is stored.
   - Media re-use: Removal of electronic PHI from electronic media before the media is made available for re-use.
   - Accountability: maintain a record of the movements of hardware and electronic media and any person responsible.
   - Data back-up and storage: Create a retrievable copy of electronic PHI when needed before movement of equipment.

Special security measures are needed on home computers that will access PHI. This includes items such as passwords to prevent access by other family members and virus protection software.

Vendor Controls

Another concern is when contractors or vendors in areas containing PHI. Diley Ridge Medical Center monitors these individuals to make sure they only have access to required information.

Technical Safeguards

Technical safeguards focus on the steps and procedures that must be in place to protect information, control access and validate the identity and authorization of users.

Some of the processes Diley Ridge Medical Center uses to promote compliance with the technical safeguard rules include the following:

- Computer system access, such as passwords
- Assigning security levels based on user identity or job responsibilities
- Proper identification of individuals and entities requesting access to PHI

Within the HIPAA requirements, it is important that individual department managers and supervisors authorize specific access for their employees. This will help to make sure the proper access is provided based upon the job duties that are assigned.

Technical Safeguards include the following five standards:

1. **Access Control**
   - Technical policies and procedures for electronic PHI systems to allow access to only those persons or software programs that have been granted access rights.
   - Unique user identification: Assign a unique username for tracking and identifying user identity.
   - Emergency access procedure: Obtain necessary electronic PHI during an emergency.
   - Automatic log-off: Electronic procedures that terminate an electronic session after predetermined time of inactivity.
   - Encryption and decryption: Mechanism to encrypt and decrypt electronic PHI.

2. **Audit Controls**
   - Implement hardware, software, and/or procedure mechanisms that examine system activity in systems that contain or use electronic PHI.
   - This includes a documented process to review computer system activity to identify abnormalities that may represent unauthorized access. Unauthorized access could be either internal (employees sharing passwords) or external (computer hackers). Audit controls allow Diley Ridge Medical Center to evaluate the programs put in place and respond to weaknesses by taking prompt corrective actions.

3. **Integrity**
   - Mechanisms to authenticate electronic PHI: Electronic mechanisms to corroborate that electronic PHI has not been destroyed or altered.

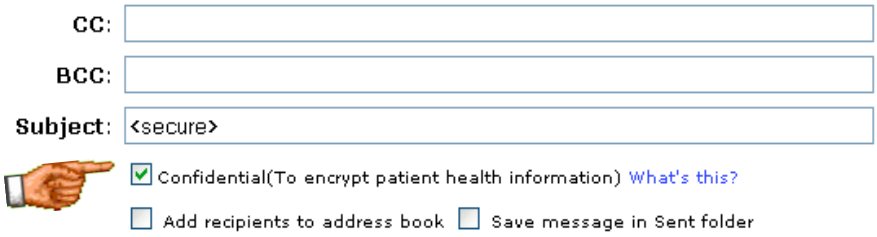
4. **Person or entity authentication**
   - Procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

5. **Transmission Security**
   - Integrity controls: Security measures that ensure electronically transmitted PHI is not improperly modified without detection until disposed of.
   - Encryption: Implement encryption of electronic PHI when appropriate.

Use of E-mail and the Internet

Disclosing patient information via e-mail must have an authorized purpose. When sending e-mail outside of the Diley Ridge Medical Center network, all e-mails that contain Diley Ridge Medical Center patient protected health information is required to be encrypted. To encrypt an e-mail message using AccessMail:

1) Create the out-bound email normally.
2) Click on the "Confidential" box.
3) Click the "Send" button to send the message.



The recipient will receive an email message which will contain a link for them to pick up the secure email message and any attachments. The recipients will be able to securely reply to your message (including attachments), which will show up in your mailbox as it normally would.

For questions about Information Security, please call Tom Enneking, Diley Ridge Medical Center Information Security Officer at 614-898-8708.