National Health Information Privacy and Security Week

Understanding the HIPAA Privacy and Security Rule

HIPAA Privacy and Security

HIPAA Privacy Rule

Final implementation April 14, 2003

- Today: Monitor compliance, continue training and improve systems

HIPAA Security Rule

Final implementation April 21, 2005

- Today: Perform risk assessment and develop plan for final implementation

Highlights of Privacy and Security Rule

- Privacy Rule
  - New Individual Rights
    - Notice of Privacy Practices
    - Amend PHI
    - Receive Accounting of Disclosures
    - Request a Restriction
    - Confidential Communication
    - File a Complaint
  - Use and Disclosure of Protected Health Information
  - Minimum Necessary
  - Policies, Procedures and Documentation

Highlights of Privacy and Security Rule

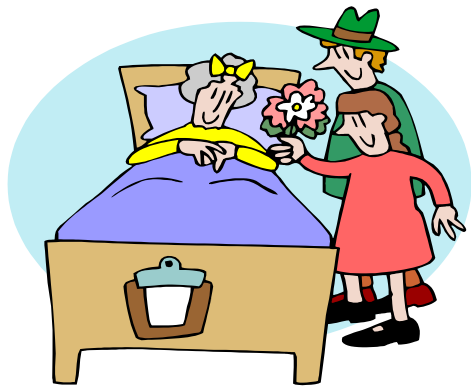
- Security Rule
  - Administrative safeguards
  - Physical Safeguards
  - Technical Safeguards
  - Organizational Requirements
  - Policies, Procedures and Documentation

The Value of HIM Professionals

Health information management professionals are protecting privacy and work to keep confidential information secure.

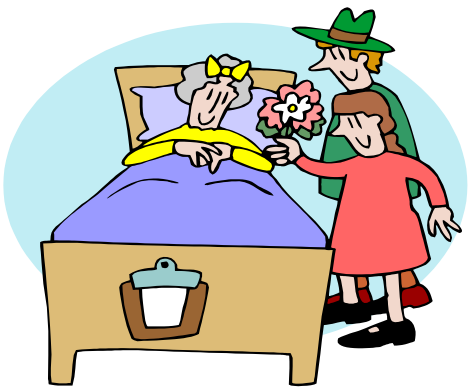
Disclosure to Family and Friends

Mrs. Jones was seeking treatment in a hospital. Her daughter frequently visits and speaks with physicians and nurses about her care.



- **Can information be disclosed without Mrs. Jones consent?**

Disclosure to Family and Friends



Yes! The privacy rule allows organizations to disclose confidential information to family and friends who are involved in care without obtaining a consent or authorization.

Professionals can use their discretion if the individual is not present or competent to agree.

Directory Information

Mrs. Jones grandson heard that his grandmother was in the hospital. He called the hospital operator to find out her condition.

- **Can her condition be disclosed?**

Directory Information

Yes! Directory information may be disclosed when the individual is asked for by name. You can disclose the location (such as room number) and condition in general terms such as good, fair, serious, or critical.

Minimum Necessary and Security Audit Controls

Mrs. Jones neighbor, who is an employee in the facility's billing office, wanted to know more about her condition. She has been an acquaintance for 20 years. Mrs. Jones son ran into her at work and told the employee she had been admitted.

- **Can the employee obtain more information on Mrs. Jones?**

Minimum Necessary and Security Audit Controls

No! Not unless she has a need to know to do her job – the minimum necessary standard applies.

The security rule requires organizations to have technical safeguards such as access controls and audit controls.

Disclosure To Other Treatment Providers

Mrs. Jones physician has requested a consultation with a specialist. He contacts the specialist to discuss the case. The specialist's office requests records from the facility prior to Mrs. Jones office visit.

- **Can they be disclosed without an authorization?**

Disclosure To Other Treatment Providers

Yes! Information may be disclosed to another treatment provider without an authorization.

The minimum necessary standard does not apply to disclosures for treatment purposes.

Fax and E-Mail

Mrs. Jones' physician and the specialist discuss the case via e-mail. The specialist's office requests the records to be faxed to assure receipt before the office visit.

- **Is this allowed?**

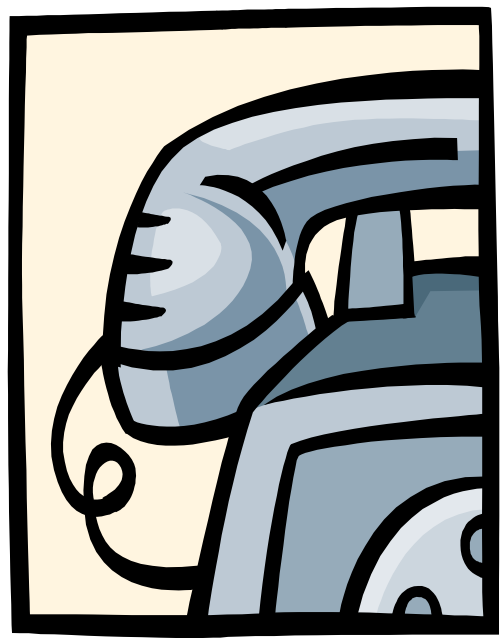
Fax and E-Mail

Yes! Neither the privacy or security rule prohibit use of e-mail or fax to transmit protected health information (PHI).

The security rule requires a covered entity to put in place appropriate safeguards (administrative, technical, physical) for ePHI that it creates, receives or transmits.

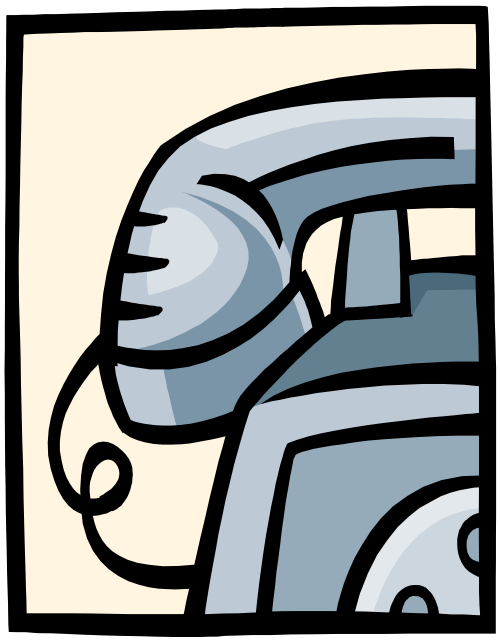
Alternate Communication and Reminders

Mrs. Jones would like appointment reminders to be called to her daughter's house. The specialist's clinic leaves a message on her daughters voicemail.



- **Is this allowed?**

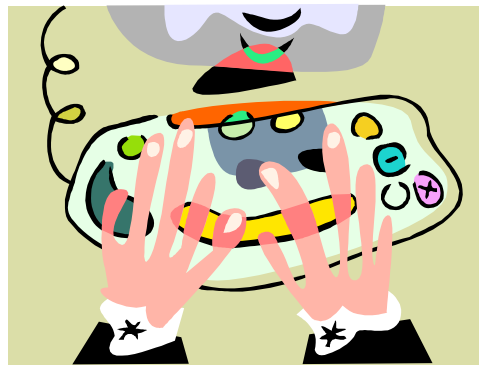
Alternate Communication and Reminders



Yes! Mrs. Jones has many rights under The privacy rule – one is the right to request communication by an alternate means. The privacy rule does not prohibit leaving a message on an answering machine but care should be taken on how much detailed information is disclosed.

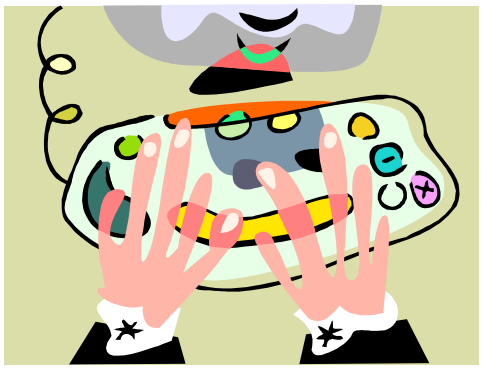
Security Controls

Mrs. Jones son, who is a lab technician, was visiting his mother and noticed the hospital had an electronic health record system. He recognized the software program, heard it was good and wanted to see how it worked. He sat down at an open PC to look at the program.



- **Should he be able to do this?**

Security Controls



No! A covered entity must have various security measures in place including:

- Technical controls on who has access into the computer system
- Physical security for the workstations
- Administrative safeguards such as policies and procedures to protect ePHI

Contingency Planning

Unfortunately, the hospital had not started planning for the HIPAA security rule and had not assessed its system vulnerabilities. Mrs. Jones' son crashed the system causing it to be down for 48 hours and lose information entered since the previous back up.

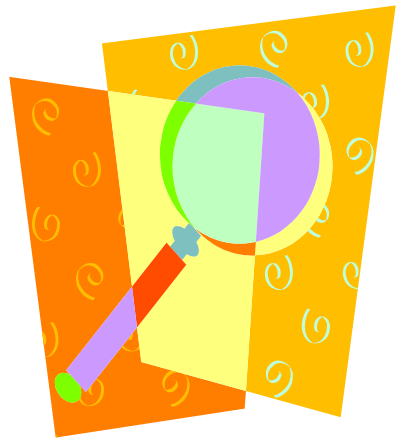
- **Could this have been prevented?**

Contingency Planning

Yes! The security rule requires HIPAA covered entities to analyze their risks and vulnerabilities. One of the areas that must be addressed is contingency planning – how to restore lost data and operate in an emergency or disaster.

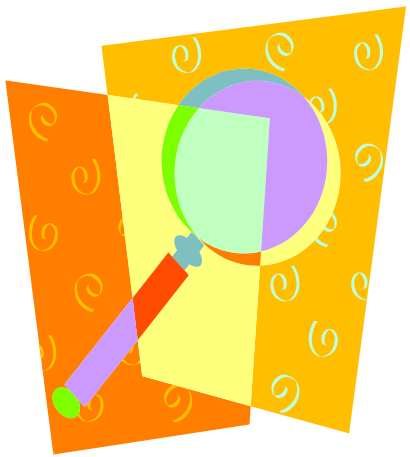
Complaint Investigation

Mrs. Jones filed a privacy complaint because her acquaintance (an employee of the hospital) told all of their neighbors why Mrs. Jones was being treated. An ensuing investigation showed through audit controls that the employee accessed Mrs. Jones confidential information.



- **Did the employee (Mrs. Jones' acquaintance) have a right to do that?**

Complaint Investigation



No! It was determined that the employee did not have a need to know.

- Individuals have the right to file a complaint with the covered entity and the Office of Civil Rights.
- Organizations must document the complaint and resolution and have a process to investigate.

Workforce Training

To address Mrs. Jones complaint, the facility agreed to retrain their workforce on privacy and security. The employee was sanctioned in accordance with facility policy.

- **Was this the appropriate way to handle the complaint?**

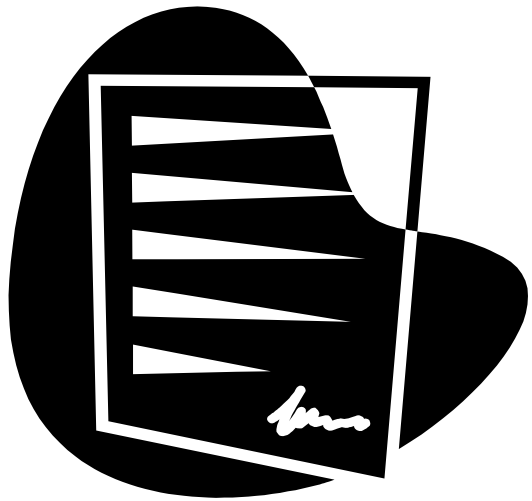
Workforce Training

Yes! Both the privacy and security rule require the work force to be trained as appropriate for their job.

Both rules also require organizations to have and enforce sanction policies.

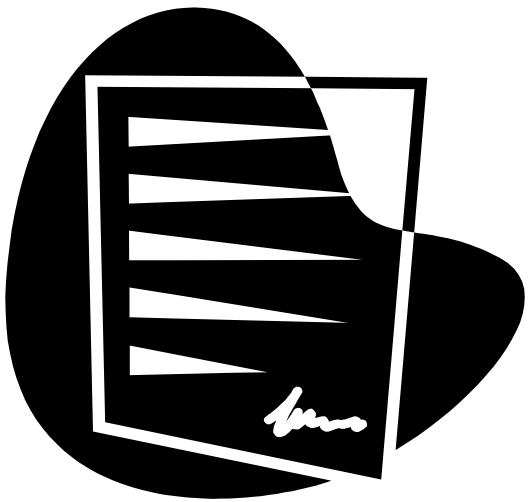
Authorization

Mrs. Jones' daughter is assisting her mother in maintaining a personal health record. She asks the HIM department for copies of important documents from her mother's medical records.



- **Is the hospital allowed to release this information to Mrs. Jones' daughter?**

Authorization



Yes, but only after Mrs. Jones signs an authorization allowing disclosure of her medical records to her daughter.

For more information on Privacy and Security visit the following online resources:

Healthcare and HIM professionals visit

www.ahima.org/hipsweek

Patients and the Public visit www.myphr.com