Electronic Medical Records:

Legal and Ethical Implications for Patients

Linda A. Simunek, RN, PhD, JD
Executive Director, Doctoral Success Grant and Adjunct Professor in Law in Healthcare Education, Fischler School of Education, Nova Southeastern University

2-11-2013

Objectives

1. Describe the duty of care owed to patients in maintaining privacy, confidentiality, and security of health care information in electronic medical records (EMR)
2. Describe the parameters for EMR patient information data sharing in a reformed health care delivery system
3. Describe the elements and penalties in criminal and civil prosecution cases for breach of health information privacy, confidentiality and security

What are Electronic Medical Records?

- Electronic Medical Records (EMR) or Electronic Health Records (EHR) are electronic, machine readable versions of much of the data found in paper-based records, comprising both structured and unstructured patient data from disparate, computerized ancillary systems and document imaging systems. Clinical documentation may originate in either paper records or computerized data; however, the data are not comprehensively coded.

(Dick, R.S. Steen E.B, and Detmer, D.E. (1997) , The computer based patient record: an essential technology for health care. Institute of Medicine, Washington: D.C)

Definition of Electronic Health Record System

- An EHR system includes:

1. Longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual or a health care provider to an individual
2. Immediate electronic access to person and population-level information by authorized, and only authorized users. (cont'd).

Definition of Electronic Health Record System

3. Provision of knowledge and decision-support that enhances the quality, safety, and efficiency of patient care, and,
4. Support for efficient processes for health care delivery

(Institute of Medicine (2003). Key capabilities of an HER system. Washington, D.C.)

Computer-based Documentation: Past, Present, and Future

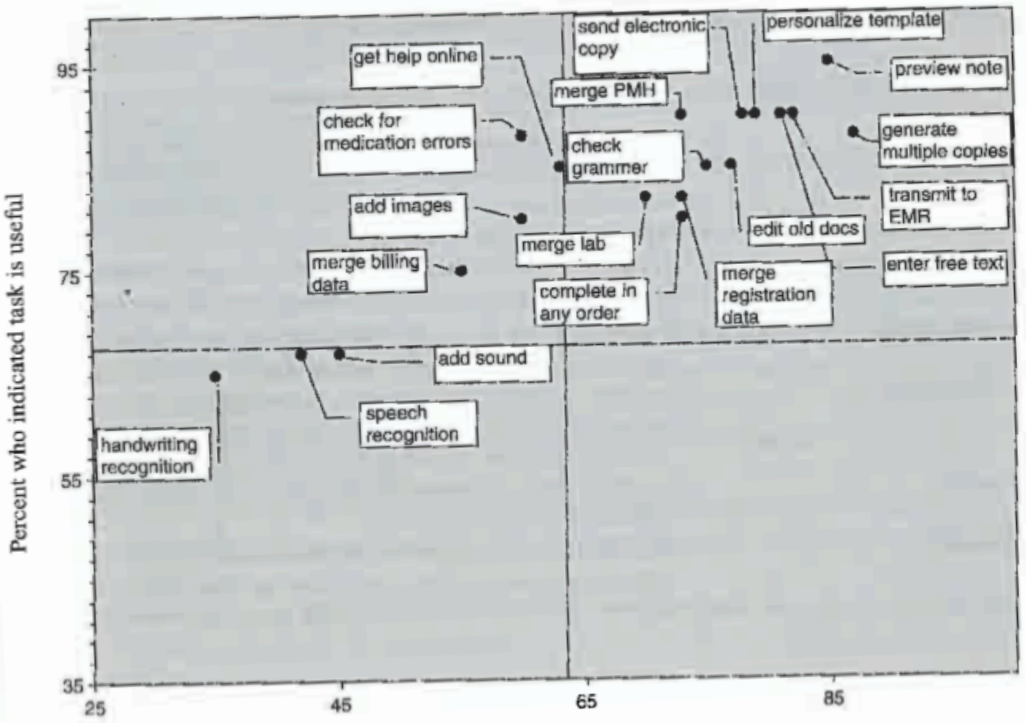

FIGURE 14-8. Summary of desired features in a CBD system.

Glossary of EMR Patients' Rights-The Right to Information Privacy

- Specific right of an individual to control the collection, use, and disclosure of personal information (Center for Technology and Democracy), (CT&D)
- A state or condition of controlled access to personal information; the ability of an individual to control the use and dissemination of information that relates to self, the individual's ability to control what information is available to various users and to limit re-disclosures of information (ASTM)

The Right to Information Privacy

- The right of individuals to keep information about themselves from being disclosed to anyone. (Computer-Based Patient Record Institute, CPRI (1994)

The Right to Confidentiality

- Tool for protecting privacy (CT&D)
- Status accorded to data or information indicating that they are sensitive for some reason and therefore need to be protected against theft, disclosure and improper use (ASTM)
- The act of limiting disclosure of private matters (CPRI)

The Right to Information Security

- Encompasses all the safeguards in an information system (CT&D)
- Totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness and oversight of these components (ASTM)
- Means to control access and protect information form accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss (CPRI)

Typical Users of Health Information

- Patient
- Primary care physician
- Health insurance company
- Clinical laboratory
- Local retail pharmacy
- Pharmacy benefits manager
- Consulting physician

Typical Users of Health Information

- Local hospital
- State bureau of vital statistics
- Accrediting organization
- Employer
- Life insurance company
- Medical Information Bureau
- Managed care company
- Attorney
- State public health and family physician
- State agency collecting hospital discharge data
- Medical researcher

Common Threats to Healthcare Information Security

- Insider accidental disclosure
- Insider abuse of access privileges
- Insider unauthorized access
- Outsider intruders

Common Threats to Information Integrity

- Insider accidental errors
- Insider malicious attack
- Intruder accidental or malicious attack
- Equipment failure
- Software failure
- Strategic attack (e.g. virus)

Common Threats to Information Reliability

- Natural hazards, earthquakes, tornadoes, ice storms, fires, floods, electrical storms, other natural disasters
- Equipment and software failures-hardware breakdowns and software failures that cause unexpected systems suspension or shutdown
- Human error-any human error that would cause hardware or software to improperly function, causing unexpected system disruption or shutdown
- Theft, malice or strategic attack, purposeful theft or attack on any component of the information system with the intent of causing system disruption or shutdown

Guiding Principles Behind HIPAA Privacy Protection

- Setting boundaries for the use of health information and imposing a legal duty of confidentiality on those who provide and pay for health care and on other entities that receive health information form them
- Requiring measures for protection of health information
- Providing consumer control over individual information
- Establishing sanctions for the misuse of information
- Balancing individual rights with the public good

Privacy Rule and Covered Entities

- A major goal of the Privacy Rule is to ensure that the individual's health information is properly protected while allowing the flow of information needed to provide and promote high quality health care and to protect the public's health and well being.

Individually Identifiable Health Information

Individually identifiable health information is information, including demographic, data that relates to:

- The past, present, or future physical or mental health or condition of an individual
- The provision of health care to the individual
- The past, present, or future payment for the provision of health care to the individual

Privacy Rule and Covered Entities

- Health plans
- Health care providers
- Healthcare clearinghouse
- Business associates

Signed authorization form for use and disclosure of protected health information (PHI)

- Description of the information to be used or disclosed
- Name of other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure
- An expiration date or event that relates to the individual or the purpose of the use or disclosure

Signed authorization form for use and disclosure of PHI

- A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke it
- A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by the privacy Rule
- Signature of the individual and date of authorization

Signed authorization form for use and disclosure of PHI

- When the authorization is signed by a personal representative of the individual, there must be a description of the representative's authority to act for the individual

Typical functions of the Chief Security Officer

- Security strategic planning
- Development of enterprise wide security policy for safeguarding the access, integrity and availability of information and information systems
- Development of enterprise-wide procedures for security policy implementation
- Coordinate the administration of security software

Typical functions of the Chief Security Officer

- Manage confidentiality agreements for employees and contractors
- Coordinate security procedures
- Coordinate employee security training
- Monitor audit trails to identify security violations
- Conduct the assessment of enterprise information systems
- Develop business continuity plan

Health Information Security Controls

- Administrative controls
- Physical controls
- Technical Controls
- Dynamic passwords
- Encryption
- Detection and intrusion systems
- Other security services

Health Information Security Checklist

- Audit Trail
  - Permits audit trail an
  - Automatic Activation
- Passwords
  - Text/Numeric
  - Biometric
    - Face
    - Voice
    - Fingerprint

Health Information Security Checklist

- Electronic Signatures
- Role-based access
- Data validation
- Back-up Process
- Encryption

Health Information Risk Analysis and Assessment

- Identifying threat or risks to security, e.g., human error such as data entry mistake, unauthorized physical access to data, sabotage, power failures, and malfunction of software or hardware
- Determining how likely it is that any given threat may occur
- Estimation of the impact of an untoward event

Policies and procedures and documentation requirements

- Covered entities must have security policies and procedures documents in written format.
- Documentation must be retained for six years from the date of the creation or the date when it was last in effect, whichever is later.

Criminal Prosecution and Case Law Examples and Analysis

- Breach of Privacy
- Breach of Confidentiality
- Breach of Security

Handout-Using the Electronic Health Record Evaluation Checklist (HER)

- Product Name
- Company
- Evaluation Date
- Chart Features-Present/Absent; Esential? Point Value
- Medication Features
- Laboratory X-ray Pathology Features
- Telephone Call Features

Handout-Using the Electronic Health Record Evaluation Checklist (HER)

- Diagnosis Features
- Referral Features
- Preventive Medicine Features
- Clinical Encounter
- Patient Education Features
- Population Health Management
- Communication and Infrastructure

Handout-Using the Electronic Health Record Evaluation Checklist (HER)

- Communications
- Decision Support
- Data Storage and File Formats
- Standards Supported
- Interface Options
- Operating Systems
- Technology

Contact Information for Linda Simunek

- Linda Agustin Simunek
- 19355 SW 25 Court
- Miramar, Florida 33029
- Monaco Cove, Gate Code 7488
- 954-830-2516 (Cell)
- 954-262-8660 (NSU Office)
- simunek@nova.edu
- lindasimunek7@gmail.com

References

- Carter, J.H. (2008). Electronic health records, American College of Physicians: Pa.
- Department of Health and Human Services. 2003.45 CFR Parts 160, 162, and 164.
  Federal Register. Vol 68, Now. 34. February 20, 2003
- Horine, G. (2005) Absolute beginner's guide to Project management ISBN23: 9780789731975
- Johns, M.L. (2003). HIPAA security: Computer based training modules. Chicago Holistic Training Solutions

Websites

- www.healthprivacy.org/usr_doc/34775.pdf
- www.privacyrights.org/ar/PharmComplaint.htm
- www.fbi.gov/page2july05/cyber072505.htm
- http://health-care-it.advanceweb.com
- www.healthmanagement.com
- www.healthcare-informatics.com
- www.ansi.org/hhitsp