TELEMEDICINE: CURRENT TRENDS AND EMERGING LEGAL RISKS PRIVACY AND SECURITY ISSUES OUTLINE

December 2008

I. Overview

A. Patient Privacy Act of 1974 – protects records maintained by governmental agencies.

B. The Joint Commission – established privacy and telemedicine standards.

C. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – mandates privacy and security standards for safeguarding electronic transactions and the electronic transmission of health information.

D. Gramm-Leach-Bliley Act of 1999 – financial institutions required to protect and safeguard data from security threats

E. Various state laws – address patient privacy, security and confidentiality concerns.

II. HIPAA Background

A. Privacy Rule – Standards for the Privacy of Individually Identifiable Health Information.

1. The Purpose:

   a. Define and limit the circumstances in which covered entities may use and disclose covered health information;

   b. Establish individual rights with respect to the covered health information; and

   c. Require covered entities to adopt safeguards to protect the confidentiality of covered health information and protect against unauthorized access.

2. "Covered Entities" include:

   a. Health plans;

   b. Health care clearinghouses; and

   c. Certain health care providers (those who transmit covered health information in connection with HIPAA standard transactions).

3. The regulations do not apply to providers who maintain a solely paper information system.

4. Subject Matter Covered:

   a. The regulations apply to "Protected Health Information." The term is defined as any individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity.

   b. Protection starts when information becomes electronic and stays with the information, so long as the information is in the hands of a covered entity.

   c. Information becomes electronic either by being sent electronically (*e.g.*, via the Internet, fax, dial-up lines, telephone voice response, etc.) or by being maintained in a computer system.

   d. The paper progeny of electronic information is covered. The information does not lose its protections simply because it is printed out of the computer.

5. Security Standards - Security Standards for the Protection of Electronic Protected Health Information.

6. Application and Purpose:

   a. Pertain to a subset of Protected Health Information referred to as "Electronic Protected Health Information" or "EPHI," which is limited to electronic forms of PHI.

   b. Require Covered Entities, in particular health care providers, to:

      (i) Ensure the confidentiality, integrity and availability of EPHI that the health care provider creates, receives, maintains, or transmits;

      (ii) Protect against any reasonably anticipated threats or hazards to the security or integrity of the information;

      (iii) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and

      (iv) Ensure compliance by the Covered Entity's workforce.

7. Implementation Specifications:

   a. Administrative safeguards;

   b. Physical safeguards; and

c. Technical safeguards.

d. Required or Addressable:

(i) If the specification is Required then the Covered Entity must implement the implementation specification.

(ii) If the specification is Addressable then a Covered Entity must:

(a) Assess whether the implementation specification is a reasonable and appropriate safeguard in its environment; and

(b) Implement the implementation specification, if it's reasonable and appropriate; or

(c) If the implementation specification is not reasonable and appropriate, then:

(1) Document why it would not be reasonable and appropriate to implement; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

B. Preemption.

1. HIPAA standards preempt state laws, which are in conflict with the regulatory requirements and that provide less stringent privacy protections.

2. Certain specified exceptions to preemption include state laws regulating public health functions, child abuse, etc.

C. HIPAA Forms

1. Notice of Privacy Practices

2. Authorizations

3. Business Associate Agreements

III. Telemedicine Privacy and Security Issues

A. Authorized disclosures of health information via telemedicine:

1. Without patient authorization (but require written informed consent under state law);

2. For treatment, payment, and health care operations;

3. For public health and law enforcement;

4. Apply minimum necessary standard.

5. Exceptions:

   a. Highly sensitive information such as psychotherapy notes requires authorization.

   b. State laws may be more stringent.

B. Providers with physician/patient relationship are responsible for the privacy and security safeguards.

C. Difficulties with compliance:

1. More risk for unauthorized access.

2. Who is responsible for notice of privacy practices?

   a. What are patients told about telemedicine?

   b. What risks are disclosed?

3. Who is responsible for providing access to health information?

4. Who is responsible for providing an accounting?

5. Tracking unauthorized disclosures.

6. Retaining medical records:

   a. Erase videotapes unless needed for documentation of abuse or neglect.

   b. Need to be concerned with document retention requirements.

   c. Who has access to medical records after termination of relationship (with patient and/or other health care provider)?

7. Who has custody of the information?

8. Traditional notions of privacy and confidentiality changed:

   a. Information shared with consulting physician.

   b. Two sets of staff and technicians.

9. Prevent unauthorized access and safeguard medical records:

a. From Internet hackers

b. Use encryption

c. Use security software

d. Use passwords

e. Trace use of information (*e.g.*, audit trails)

f. De-identify information when possible

D. Specific policies and procedures

E. Training

F. Monitor compliance

G. Contractual arrangements:

1. Confirm contracts hold parties accountable.

2. Who has custody of the information?

3. Become familiar with the other party's policies and procedures.

4. What state/nation's law applies.

5. Types of contracts:

a. Telemedicine agreements

b. Vendor contracts

c. Business associate agreement

d. Privacy and confidentiality agreements

H. Concerns:

1. Limiting information prevents unauthorized disclosures but may preclude quality care.

2. Need for more guidance.

I. Liability

1. Federal, State and International

2. Breach of confidentiality for improper disclosures and access:

   a. Loss of job
   b. Loss of reputation
   c. Loss of health insurance
3. Destruction of integrity of information
4. Malpractice
5. Civil and criminal penalties
6. Imprisonment