Chapter 9
Legal Aspects of Health Information Management

EXERCISE 9-1 Legal and Regulatory Terms
1. T
2. F
3. F
4. F
5. F

EXERCISE 9-2 Maintaining the Patient Record in the Normal Course of Business
1. hearsay, Uniform Business Records
2. electronic
3. transmission
4. state laws
5. Safeguards for records:
   a. Created by a person within the business who has knowledge of the acts, conditions, diagnoses, events, or opinions documented
   b. Documented in the normal course of business
   c. Generated at or near the time of patient care
   d. Maintained in the regular course of business
Additional safeguards include:
   e. Using a computer that is accepted as standard and efficient equipment
   f. Documenting the method of operation used to create an electronic medical record
   g. Documenting the method and circumstances of preparing the record includes sources of information on which the record is based
   h. Implementing procedures for entering information into and retrieving information from the computer, controls and checks used, and tests performed to ensure the accuracy and reliability of the record
   i. Ensuring that information documented in the EMR has not been altered in any way
   j. Maintaining records at an off-site backup storage system in case the on-site system is damaged or destroyed
k. Using an imaging system to copy documents that contain signatures, ensuring that records, once in electronic form, cannot be altered
l. Safeguarding the confidentiality of records and preventing access by unauthorized persons
m. Allowing authentication of record entries via electronic signature keys, and implementing procedures for system maintenance

EXERCISE 9-3 Confidentiality of Information and HIPAA Privacy and Security Provisions

1. F
2. T
3. F
4. T
5. F

EXERCISE 9-4 Legislation that Impacts Health Information Management

1. Drug Abuse and Treatment Act of 1972
2. Health Care Quality Improvement Act of 1986
3. Omnibus Budget Reconciliation Act of 1987
4. Healthcare Integrity and Protection Data Bank
5. Health Insurance Portability and Accountability Act of 1996

EXERCISE 9-5 Release of Protected Health Information

1. Miss Molly should first determine how the patient is being transported to Pathway Drug and Alcohol Rehabilitation Center. If the patient is being transported by New Directions Medical Center, a copy of the report should be placed in a sealed envelope and given to the staff member accompanying the patient to the Pathway Drug and Alcohol Rehabilitation Center. The staff member should hand over the report to the registration clerk at the Pathway Drug and Alcohol Rehabilitation Center; the report will be placed in the patient record created at that facility. If the patient is transported privately to Pathway Drug and Alcohol Rehabilitation Center, HIPAA provisions allow for release of the report. Faxing the report in this situation is appropriate because the Pathway Drug and Alcohol Rehabilitation Center needs access to that information to develop a treatment plan for the patient (even though this situation is not an emergency). Note: Most health care facilities continue to obtain patient authorization to release protected health information (PHI) even though HIPAA provisions clearly state that release of PHI to a treating provider is permitted so continuity of care can be facilitated.

2. Ms. Marie should use the “call-back method” to respond to this request, which involves obtaining the requesting provider’s main switchboard number from the phonebook or directory assistance, calling that number, and asking to be connected to the department (or provider) requesting the PHI to ensure that she is speaking with an individual authorized to obtain the information. Note: Most health care facilities continue to obtain patient authorization to release protected health information (PHI) even though HIPAA provisions clearly state that release of PHI to a treating provider is permitted so continuity of care can be facilitated. In no circumstances should Ms. Marie contact the patient’s family. This would be considered a breach of confidentiality and illegal under HIPAA provisions.

3. Pam should not respond to the patient via email because this form of communication is not secure. (Emails are not usually encrypted.) Pam should arrange to have the provider call the patient with the lab results.
CHAPTER REVIEW
Short Answer
16. Civil monetary penalties include $100 per violation, up to $25,000 per person/per year for each requirement or prohibition violated. Federal criminal penalties include up to $50,000 and one year in prison for obtaining or disclosing protected health information, up to $100,000 and up to five years in prison for obtaining protected health information under “false pretenses,” and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

17. Administrative law includes regulations created by administrative agencies of government. Case law is based on judicial decisions and precedent rather than on statutes. Statutory law is passed by a legislative body, and it can be amended, repealed, or expanded by the legislative body.

18. For records to be admissible the records must be:
   a. Created by a person within the business who has knowledge of the acts, conditions, diagnoses, events, or opinions documented
   b. Documented in the normal course of business
   c. Generated at or near the time of patient care
   d. Maintained in the regular course of business

19. Protected health information is information that is identifiable to an individual, such as name, address, telephone numbers, social security number, diagnosis, medical record number, and information contained in a patient’s record.

20. Covered entities should establish administrative, physical, and technical safeguards.

<table>
<thead>
<tr>
<th>Administrative Safeguards</th>
<th>Implementation Specifications for Covered Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security management process</td>
<td>Policies and procedures to prevent, detect, contain, and correct security violations include:</td>
</tr>
<tr>
<td></td>
<td>• Risk analysis (assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI)</td>
</tr>
<tr>
<td></td>
<td>• Risk management (implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level)</td>
</tr>
<tr>
<td></td>
<td>• Sanction policy (apply appropriate penalties against workforce members who fail to comply with the security policies and procedures of the covered entity)</td>
</tr>
<tr>
<td></td>
<td>• Information system activity review (implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports)</td>
</tr>
</tbody>
</table>

Assigned security responsibility

Identify the security official responsible for development and implementation of security policies and procedures.

Workforce security

Ensure that all workforce members have appropriate access to electronic PHI, and prevent those workforce members who do not have access from obtaining access to electronic PHI:
- Authorization and supervision of workforce members who work with electronic PHI or in locations where PHI might be accessed
- Workforce clearance to determine that the access of a workforce member to electronic PHI is appropriate
• Terminating access to electronic PHI when the employment of a workforce member ends

Information access management

Authorizing access to electronic PHI:
• Isolating health care clearinghouse functions if a health care clearinghouse is part of a larger organization; the clearinghouse must implement policies and procedures that protect electronic PHI of the clearinghouse from unauthorized access by the larger organization
• Authorizing access to electronic PHI (e.g., workstation)
• Establishing and modifying access to a workstation, transaction, program, or process

Security awareness and training

Security awareness and training program for all workforce members:
• Security reminders via periodic security updates and protection from malicious software to guard against, detect, and report malicious software
• Log-in monitoring to investigate log-in attempts and report discrepancies
• Password management to create, change, and safeguard passwords

Security incident procedures

Address security incidents through response and reporting:
• Identify and respond to suspected or known security incidents
• Mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity
• Document security incidents and their outcomes

Contingency plan

Respond to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems containing electronic PHI:
• Data backup plan to create and maintain retrievable exact copies of electronic PHI
• Disaster recovery plan to restore any loss of data
• Emergency mode operation plan to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode
• Testing and revision procedures for periodic testing and revision
• Applications and data criticality analysis to assess the relative criticality of specific applications and data in support of other contingency plan components

Evaluation

Perform periodic technical and nontechnical evaluations, based initially upon the standards implemented under this rule, and, subsequently, in response to environmental or operational changes affecting the security of electronic PHI, which establishes the extent to which an entity’s security policies and procedures meet security requirements.

Associate contracts and other
Permit a business associate to create, receive, maintain, or transmit arrangements electronic PHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

Physical Safeguards

Facility access controls

Limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed:

- **Contingency operations** to allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency
- **Facility security plan** to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft
- **Access control and validation procedures** to control and validate a person’s access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision
- **Maintenance records** to document repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks)

Workstation use

Specify proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

Workstation security

Physical safeguards for all workstations that access electronic PHI to restrict access to authorized users.

Device and media controls

Govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility:

- **Disposal** of electronic PHI and the hardware or electronic media on which it is stored
- **Media re-use** to remove electronic PHI from electronic media before the media are made available for re-use
- **Accountability** to maintain a record of the movements of hardware and electronic media and any person responsible therefore
- **Data backup and storage** to create a retrievable, exact copy of electronic PHI, when needed, before relocating equipment

Technical Safeguards

Access control

Maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights:

- **Unique user identification** to assign a unique name and number for identifying and tracking user identity
• **Emergency access procedure** to obtain necessary electronic PHI during an emergency
• **Automatic logoff** electronic procedures that terminate an electronic session after a predetermined time of inactivity
• **Encryption and decryption** mechanism to encrypt and decrypt electronic PHI

**Audit controls**
Hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

**Integrity**
Protect electronic PHI from improper alteration or destruction:
• **Mechanism to authenticate electronic PHI** to corroborate that information has not been altered or destroyed in an unauthorized manner

**Person or entity authentication**

**Transmission security**
Verify that a person or entity seeking access to electronic PHI is the one claimed. Technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network:
• **Integrity controls** to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.
• **Encryption mechanism** to encrypt electronic PHI whenever deemed appropriate

**Business associate contracts or other arrangements**
Contracts or other arrangements between the covered entity and its business associate must meet HIPAA requirements.

**Requirements for group health plans**
Ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic PHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

**Policies and procedures**
Comply with the standards, implementation specifications, or other requirements of the security rule.

**Documentation**
Comply in written (which may be electronic) form; and if an action, activity, or assessment is required to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment:
• **Time limit** to retain required documentation is for six years from the date of its creation or the date when it last was in effect, whichever is later
• **Availability**—documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains
• **Updates**—documentation must be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of the electronic PHI