

Healthcare Privacy, Confidentiality, Legal, and Ethical Issues

© saatchi/shutterstock, Inc.

CHAPTER

3

1. Introduction to the Legal System

- a. The legal system is the system of principles and processes by which people who live in a society deal with their disputes and problems, seeking to solve or settle them without resort to force. Laws govern the relationships among private individuals, organizations, and government. The legal system is a combination of private and public law.

- i. Private

- 1. Also considered civil law
 - 2. Concerned with the recognition and enforcement of the rights and duties of private individuals and organizations (i.e., patient and healthcare facility)
 - 3. Legal issues between private parties are torts and contracts
 - a. Tort
 - i. An injury or wrong committed against an individual or his property
 - ii. In tort action, one party asserts that wrongful conduct on the part of another caused harm and seeks compensation for the harm suffered.
 - b. Contract
 - i. Concerned with legally enforceable agreements between two or more individuals
 - ii. In contract disputes, one party asserts that in failing to fulfill an obligation, the other party breached a contract, and the asserting party seeks either compensation or performance of the obligation as a remedy.
 - iii. Court order: one party forces the breaching party to fulfill its alleged obligation.

- ii. Public

- 1. Deals with the relationships between private parties and the government; consists of rules, criminal law, and government regulations
 - a. Criminal
 - i. Prohibits conduct considered injurious to society as a whole and provides for punishment of those found to have engaged in such conduct
 - ii. Crime versus tort
 - 1. Crime is an offense against a person or the public at large.
 - 2. Tort is a civil wrong against an individual.

- b. Regulations
 - i. Multiple government regulations require private individuals and organizations to follow specified courses of action in connection with their activities.
 - c. Rule: a principle or regulation that governs an action, conduct, or procedure.
- iii. Sources of law. There are four main law affecting healthcare system.
 - 1. Constitution
 - a. Supreme law of the land: supreme, highest law in the United States
 - b. Establishes the general organization of the federal government, and grants certain powers to and places limits on the three branches of the federal government (executive, legislative, judicial)
 - c. Each state has its own constitution.
 - i. Express power: stated in Constitution (e.g., power to tax)
 - ii. Implied power: not stated in Constitution. They are actions considered necessary and proper to permit Express power to be accomplished.
 - d. Each city has its own charter.
 - e. Constitution places limit on what state and federal government can do
 - i. Constitutional right important to health care
 - a. Due process (right to be fully heard)
 - b. Right of privacy
 - c. Right to be left alone
 - f. Constitution overrides state and federal lower laws that are deemed unconstitutional
 - 2. Statutes
 - a. Statutory or codified law refers to written laws or statutes enacted by such bodies as the United States Congress and state and local legislatures.
 - b. Constitutional and federal law take precedence over conflicting state laws, and state laws take precedence over conflicting local government rules.
 - c. Examples of federal laws affecting healthcare facilities
 - i. American Recovery and Reinvestment Act
 - ii. Safe Medical Devices Act
 - iii. Americans with Disabilities Act
 - 3. Decisions of the court
 - a. Common law or uncodified law derived from the common law of England applied to the courts of the United States
 - b. Consist of principles that have evolved over time from court decisions resolving controversies
 - c. When a case decision is considered to serve as an authority or example for subsequent similar or identical cases, the case is said to have set a legal precedent.
 - 4. Rules of administrative agencies
 - a. Legislatures have delegated to administrative agencies the responsibility and power to implement various laws (e.g., DHHS).

- b. The delegated powers include quasi-legislative power to adopt regulations and the quasi-judicial power to decide how the statutes and regulations apply to individual situations.
 - c. Legislatures delegate these powers because legislators do not have the time or expertise to address the complex issues involved in some areas that need to be regulated.
 - b. Branches of the Government (Federal and State)
 - i. Executive (president or governor)
 - 1. Enforces and administers the law
 - 2. United States Constitution invests this power in the president, who is the administrative head of the executive branch.
 - 3. Oversees various agencies, including DHHS, which manages CMS
 - ii. Legislative (Congress and state legislatures)
 - 1. Enacts laws
 - 2. Creates new legislation, amends or repeals existing legislation
 - 3. Federal and state levels (except Nebraska, which has only one house) consist of two houses, one composed of senators and the other representatives.
 - iii. Judicial (U.S. Supreme Court, various state and federal courts)
 - 1. Responsible for interpreting the law through hearing and resolving disputes in accordance with the law
 - 2. Three sources of judicial power
 - a. Federal courts
 - i. Have jurisdiction over
 - 1. Cases involving questions of federal law
 - 2. Treaties
 - 3. Cases concerning maritime matters
 - 4. Cases that involve two or more states
 - ii. Federal court system structure
 - 1. District courts (trial courts)
 - 2. Courts of appeal
 - 3. Supreme Court
 - b. State courts
 - i. Vary by state but can be divided into four general categories
 - 1. Trial courts of limited jurisdiction
 - 2. Trial courts of general jurisdiction
 - 3. Intermediate appellate courts
 - 4. Courts of last resort (supreme courts)
 - c. Administrative agencies
 - i. Empowered by law to make regulations with the force of the law, and can also conduct hearings and take measures to enforce these regulations (e.g., Food and Drug Administration, and Centers for Medicare and Medicaid services, and Internal Revenue Services)
 - 3. Each level of government (federal, state) has its own set of courts.
 - a. Courts have different jurisdiction based upon geographical area, area of authority, and type of case.
 - b. Trial and appellate courts
 - i. Trial courts initially hear a case and pass judgment (original jurisdiction).
 - ii. Litigants unsatisfied with trial court decisions may appeal their case to appellate courts (court of appeals).

Table 3-1 Federal and State Court Sequences of Appeals

Level of Court	Federal	State
Highest appellate courts	U.S. Supreme Court (may consider appeals from state supreme courts on federal questions)	State supreme courts
Appellate courts	U.S. Court of Appeals	Circuit courts, district courts, and courts of common pleas
Special jurisdiction courts	U.S. Customs, Claims, and Tax	
Trial courts	U.S. District Courts	District, probate, family, criminal courts
Lower local courts (non-jury)		Traffic, police, small claims, Justice of Peace

1. Two types of review (see Table 3-1)
 - a. Error correction monitors decisions of lower trial courts for proper application and interpretation of law; does not seek new evidence, but examines records of lower courts for errors.
 - b. Sort cases for Supreme Court review
 - c. Court interpret statutes and regulations, decide validity, follow precedent, or create common law (case law)
 - d. When no statutes or regulation apply, courts adhere to principle of “let the decision stand” (stare decisis)

2. Health Record Requirements and Retention Guidelines

- a. Record Requirements
 - i. Federal and state laws and regulations provide guidance as to patient record content, privacy, and security.
 - ii. Some state laws and regulations specify that health records must be maintained by healthcare institutions and that the information must be kept confidential.
 - iii. Most state law expressly allows a patient or authorized representative to inspect the health record (typically, a written request must be made and reasonable cost paid).
 - iv. State licensing laws usually address at least the minimum content of a health record.
 - v. In addition to federal, state, and local laws, numerous nongovernmental agencies specify standards for healthcare facilities (e.g., TJC).
 - vi. TJC, American Osteopathic Association (AOA), Medicare/Medicaid Conditions of Participation (CoP), and other accrediting bodies provide standards for patient recordkeeping.

1. There should be one record per patient, with the following contents for an inpatient record:
 - a. History and physical
 - b. Documentation of infections and complications
 - c. Consent forms
 - d. Notes, reports, ancillary reports
 - e. Discharge summary
 - f. Final diagnosis
2. Outpatients:
 - a. Encounter note
 - b. Consent forms
 - c. Diagnostic testing
 - d. Presumptive diagnosis
 - e. Medication reconciliation
 - f. Allergies/Drug interaction
- vii. CMS published meaningful use rules
 1. Meaningful use: set of standards defined by the Centers for Medicare and Medicaid Services (CMS) Incentive Programs that governs the use of electronic health records and allows eligible providers and hospitals to earn incentive payments by meeting specific criteria (Table 3-2).
 2. The goal of meaningful use is to promote the spread of electronic health records to improve health care in the United States.
 - a. HITECH Act is a part of American Recovery and Reinvestment Act (ARRA)

Table 3-2 Meaningful Use Criteria

Stage 1: Meaningful use criteria focus on:	Stage 2: Meaningful use criteria focus on:	Stage 3: Meaningful use criteria focus on:
Electronically capturing health information in a standardized format	More rigorous health information exchange (HIE)	Improving quality, safety, and efficiency, leading to improved health outcomes
Using that information to track key clinical conditions	Increased requirements for e-prescribing and incorporating lab results	Decision support for national high-priority conditions
Communicating that information for care coordination processes	Electronic transmission of patient care summaries across multiple settings	Patient access to self-management tools
Initiating the reporting of clinical quality measures and public health information	More patient-controlled data	Access to comprehensive patient data through patient-centered HIE
Using information to engage patients and their families in their care		Improving population health

Reproduced from HealthIT.gov. EHR Incentives & Certification: Meaningful Use Definition & Objectives. <http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives>. Accessed March 4, 2014.

- b. Allocates \$19 billion for health information technology incentive
 - c. Incentives meant to reward hospital and eligible professionals who are meaningful users of certified electronic health records
 - d. CMS published Proposed Rule for Meaningful Use Stage 1 on December 31, 2009
 - e. CMS issued Final Rule on July 13, 2010
- 3.** Benefits of the meaningful use of EHRs:
- a. Complete and accurate information
 - i. With electronic health records, providers have the information they need to provide the best possible care.
 - ii. Providers will know more about their patients and their health history before they walk into the examination room.
 - b. Better access to information
 - i. Electronic health records help providers access information needed to diagnose health problems earlier and improve the health outcomes of their patients.
 - ii. Electronic health records allow information to be shared more easily among doctors' offices, hospitals, and across health systems, leading to better coordination of care.
 - c. Patient empowerment
 - i. Electronic health records empower patients to take a more active role in their health and in the health of their families.
 - ii. Patients can receive electronic copies of their medical records and share their health information securely over the Internet with their families.
- 4.** Stages of meaningful use
- a. To achieve meaningful use, eligible providers and eligible hospitals must adopt certified EHR technology and use it to achieve specific objectives.
 - b. Meaningful use objectives and measures will evolve in three stages over the next 5 years:
 - i. Stage 1 (2011–2012): data capture and sharing
 - ii. Stage 2 (2014): advance clinical processes
 - iii. Stage 3 (2016): improved outcomes
 - c. Achieving meaningful use during stages requires meeting both core and menu objectives.
 - i. All of the core objectives are required.
 - ii. Eligible providers and hospitals may choose which objectives to meet from the menu set.
- 5.** Eligible hospital objectives
- a. Improve quality, safety, efficiency, and reduce health disparities
 - i. Clinical patient order entry
 - ii. Drug–drug and drug–allergy checks
 - iii. Drug–formulary checks
 - iv. Problem list
 - v. E-prescribing
 - vi. Active medication list
 - vii. Medication allergy list
 - viii. Patient demographics

- ix. Vital, BIM, and growth chart
 - x. Smoking status
 - xi. Incorporate clinical lab test results
 - xii. Generate lists of patient
 - xiii. Report on quality measures
 - xiv. Send reminders to patient
 - xv. Clinical decision support
- b. Engage patients and families
 - i. Electronic copy of health information
 - ii. Electronic access for patients
 - iii. After-visit summary
 - iv. Patient education
- c. Improve care coordination
 - i. Exchange key clinical information electronically
 - ii. Medication reconciliation
 - iii. Summary of care
- d. Improve population and public health
 - i. Submit data to immunization registries
 - ii. Send syndromic surveillance data to health agencies
- e. Ensure adequate privacy and security of protections for personal health information
 - i. Protect electronic health information
- b. Reporting Requirements
 - i. In certain circumstances, federal and state law allows healthcare organizations to disclose confidential information without the patient's consent.
 - 1. Child abuse
 - 2. Abuse of adults and injuries to disabled persons
 - 3. Abortions
 - 4. Cancer
 - 5. Death or injury from use of a medical device
 - 6. Communicable diseases, including HIV/AIDS, tuberculosis, etc.
 - 7. Gunshot wounds
 - 8. Birth and death
 - ii. Categories 1–8 do specify what can be reported without the consent of the patient due to state and federal law.
 - iii. Except as otherwise permitted by law, anything outside of this cannot be disclosed unless the patient consented to the disclosure.
- c. Retention Guidelines
 - i. Forces influencing retention of health information are as follows:
 - 1. Healthcare providers' ability to
 - a. Render continuing patient care
 - b. Conduct education and research
 - c. Defend a professional liability action
 - 2. Storage constraints
 - 3. Historical value
 - 4. Research and education
 - 5. Medium for storing records
 - 6. New technology
 - 7. Fiscal concerns
 - ii. Retention schedule as recommended by AHIMA.

d. Record Destruction

- i. Instances of health record destruction**
 - 1. In ordinary course of business**
 - 2. Provider's closure**
- ii. Institution should have a policy addressing the controlling statute or regulation governing when a health record may be destroyed.**
- iii. Records may be destroyed through shredding, burning, or some other means.**
- iv. Some states require facility to maintain an abstract of patient data prior to destroying, or may require patient to be notified that his or her record will be destroyed.**
- v. Facilities should maintain a permanent, dated, certified log of evidence of patient records that have been destroyed in the ordinary course of business.**

3. Confidentiality, Consent, and Security of Health Records

- a. Creation of health record is the responsibility of healthcare facility and those who provide care to the patient.**
- b. Ownership of Health Record**
 - i. Physical health record is the property of the healthcare provider, physician, or hospital that maintains it, because it is the healthcare provider's business record.**
 - ii. Patients have limited rights to access and control the disclosure of their information.**
 - iii. The patient and others have an interest in the information contained within the health record.**
 - iv. The patient and others as authorized have the right to access the information but do not have a right to possess the physical record.**
- c. Confidentiality**
 - i. Privacy is the right of an individual to be left alone.**
 - ii. Information derived from a clinical relationship between patients and healthcare professionals is patient-specific health information.**
 - 1. Healthcare providers should protect patient-specific health information from disclosure.**
 - iii. Confidential communication is information given in the belief that it will not be disclosed to another party.**
 - iv. Confidentiality after death**
 - 1. Patient's personal representative or the executor of the patient's estate may waive privilege.**
- d. Privileged Communication**
 - i. Special relationship between patient and healthcare provider**
 - ii. Three elements of privileged communication**
 - 1. Relationship between patient and provider**
 - 2. Information must have been acquired through such a relationship.**
 - 3. Information must have some connection with the provider's task of treating the patient.**
- e. Types of Consent**
 - i. Do not resuscitate**
 - 1. Tells medical professionals not to perform cardiopulmonary resuscitation (CPR) if the patient's breathing or heartbeat stops**
 - 2. An adult patient may consent to DNR through a healthcare proxy or durable power of attorney.**
 - ii. Admission includes generalized consent that documents a patient's consent to receive medical treatment at the facility.**

- iii. Release of information is consent for provider to release healthcare information for the purpose of reimbursement, continuity of care, or other reason, as authorized by the patient or patient's legal representative.
- iv. Informed consent (treatment and surgery)
 - 1. Process of advising a patient about treatment options and, depending on state laws, the provider may be obligated to disclose a patient's diagnosis, proposed treatment/surgery, reason for treatment/surgery, possible complications, likelihood of success, alternative treatment options, and risks if the patient does not undergo treatment/surgery
 - 2. Should include an explanation of the risks and benefits of treatment/surgery, alternatives, and evidence that the patient or appropriate legal representative understands and consents to the treatment/surgery
 - 3. TJC standards require that a patient consent to treatment and that the record contain evidence of consent.
 - 4. AOA requires a dated, timed, and signed informed consent for surgery on the patient's chart prior to surgery being performed.
 - 5. Medicare CoP state that all records must contain written patient consent for treatment and procedures specified by the medical staff, or by federal or state law
- f. Advance Directive
 - i. As part of the Omnibus Budget Reconciliation Act of 1990, the U.S. Congress passed the Patient Self-Determination Act. The act required providers participating in the Medicare and Medicaid programs to inform patients of their rights to express written preferences regarding healthcare decisions to be followed if the patient becomes unable to make or communicate decisions, such as a decision to withdraw life support systems.
 - ii. Legal document in which patients provide instructions as to how they want to be treated in the event they become very ill and there is no reasonable hope for recovery
- g. Durable Power of Attorney
 - i. Legal document in which patients name someone close to them to make decisions about their health care in the event they become incapacitated
 - ii. The durable power of attorney holder has the permission to request and receive information about the patient as detailed in the durable power of attorney.
 - iii. Uniform Health Care Decisions Act (UHCDA): priority order list
 - a. Spouse
 - b. Adult child
 - c. Living parents
 - d. Adult sibling
 - e. Not-related adult who has exhibited special care and concern for the individual
 - f. Healthcare provider may see court appointment.
 - iv. Also called a healthcare proxy
- h. Security of Health Records
 - i. Organizations must maintain the physical and electronic protection of the integrity, availability, and confidentiality of computer-based information and the resources used to enter, store, process, and communicate it.

- ii. Security of paper-based health records
 1. Maintain secure from unauthorized access
 2. Utilize a tracking system to locate records
 3. Educate personnel on confidentiality of patient information
 - iii. Records must be protected from loss, theft, tampering, and destruction.
- 4. Laws and Regulations Regarding Health Records**
- a. Statute of Limitations
 - i. Legislatively imposed time constraints that restrict the period of time after the occurrence of an injury during which a legal action must be commenced
 - ii. Should a cause of action be initiated later than the time prescribed, the case cannot proceed.
 - iii. The statutory period begins when an injury occurs, although in some cases (usually involving foreign objects left in the body during surgery) the statutory period commences when the injured person discovers or should have discovered the injury.
 - iv. The statute of limitation of health records varies by state. However AHIMA and the AMA offer guidelines for record retention. Adult health records should be retained for 10 years while minor health records until the age of majority plus the state statute of limitation. Immunization records, birth, death and surgical registers and the Master Patient Index should be maintained indefinitely. AMA states Medicare or Medicaid health records should be kept at least five years but AHIMA recommends the adult and minor health record retention guidelines regardless of payor. In order to preserve confidentiality when discarding records, all documents should be destroyed with the institution keeping a ledger of all records destroyed. The AMA suggests informing patients before discarding old records to give them the opportunity to claim their records or have them sent to another physician.
- 5. Release of Information and Subpoenas**
- a. Release of Information
 - i. Patient or legal representative may authorize disclosure of patient's healthcare information unless it would be in the patient's best interest not to have such information disclosed, such as psychiatric information.
 - ii. The patient or legal representative controls access by all third parties except those to which the healthcare institution is required to report information of a medical nature or as otherwise provided by law.
 - b. Subpoena
 - i. Court order requiring someone to appear in court to give testimony
 - ii. Disregarding a subpoena can result in contempt of court.
 - iii. Common elements of valid subpoena
 1. Name of court where lawsuit is brought
 2. Names of parties to the lawsuit
 3. Docket number of the case
 4. Date, time, and place of the requested appearance
 5. Specific documents to be produced if a subpoena duces tecum is involved
 - a. Subpoena duces is a written order commanding a person to appear, give testimony, and bring all documents (records) described in the subpoena to court.
 6. Name and telephone number of attorney who requested the subpoena

Table 3-3 Federal Laws and Regulations for Health Information

Legislation	Summary
Drug Abuse and Treatment Act (1972)	Requires drug and alcohol abuse patient records to be kept confidential and not subject to disclosure except as provided by law.
Emergency Medical Treatment and Active Labor Act of the Consolidated Omnibus Budget Reconciliation Act (1985)	Hospitals and physicians who participate in the Medicare program must follow certain guidelines for the treatment and transfer of all patients, regardless of patient participation and eligibility for Medicare. Also referred to as antidumping law.
Federal Tort Claims Act (1946)	The U.S. government's immunity from tort liability was largely abolished and certain conditions for suits and claims against the U.S. government were established.
Freedom of Information Act (1966)	Individuals can seek access to information without the authorization of the person to whom the information applies when the information is held by a federal agency (except personal records such as medical records).
Health Care Quality Improvement Act (1986)	Established the National Practitioner Data Bank (NPDB), which contains information about practitioner's credentials, including previous medical malpractice payment and adverse action history.
Health Insurance Portability and Accountability Act (1996)	Mandated administrative simplification regulations that govern privacy, security, and electronic transactions standards for healthcare information.

- 7. Signature, stamp, or seal of the official empowered to issue the subpoena
- 8. Witness fees, where provided by law
- iv. Contempt of court
 - 1. Results when a person fails to obey a subpoena and is punishable by fine or imprisonment
- v. Subpoena ad testificandum
 - 1. Court order that requires a person to appear in court to testify
- vi. Subpoena duces tecum
 - 1. Court order that commands a person to come to court and produce whatever documents are named in the order
- 6. Healthcare Privacy
 - a. The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") established, for the first time, a set of national standards for the protection of certain health information.

Table 3-4 Federal and State Legislation Relevant to Health Care and Maintenance of Health Records

Legislation	Summary
Patient Self-Determination Act (1990)	Requires that all healthcare facilities notify patients age 18 and over that they have the right to have an advance directive placed in their medical record. Facilities must inform patients, in writing, of state laws and facility policies regarding implementation of advance directives. The patient record must document whether the patient has executed an advance directive. Allows a person to: <ol style="list-style-type: none"> 1. Make decision concerning medical care 2. Accept or refuse treatment 3. Present their request for treatment at time of admission (administrative directive or living will)
Privacy Act (1974)	Gives individuals some control over the information collected about them by the federal government; under this act, people have the right to: <ol style="list-style-type: none"> 1. Learn what information has been collected about them 2. View and have a copy of that information 3. Maintain limited control over the disclosure of that information to other persons or entities
Occupational Safety and Health Act (1970)	Created the Occupational Safety and Health Administration (OSHA), whose mission is to ensure safe and healthy workplaces.
Omnibus Budget Reconciliation Act (1987)	Created the Nursing Home Reform Act, which ensures residents of nursing homes receive quality care, requires provision of certain services, and establishes a residents' bill of rights.
Omnibus Budget Reconciliation Act (1990)	Requires reporting of adverse actions to the Centers of Medicare and Medicaid Services (CMS) and to state medical boards and licensing agencies.
Tax Equity and Fiscal Responsibility Act (1982)	TEFRA introduced the Peer Review Organization (PRO) program as a component of Medicare law to ensure the quality of care rendered to patients.
Uniform Business Records as Evidence Act (1936)	Stipulates that records can be admitted as evidence in a court of law if they were kept in the ordinary course of business. As of 1995, 46 of the 50 states had adopted it.
Uniform Healthcare Information Act (1985)	Serves as a model for state adoption and provides rules about health information management. As of 1996, only Montana and Washington had enacted this model legislation.

Table 3-5 Landmark Cases

Case	Court Decision
<i>Behringer vs. Medical Center at Princeton</i> (1991)	News of a physician on staff at the hospital where he was treated and diagnosed with AIDS was circulated among staff and patients. Physician sued the hospital for breach of duty to maintain confidentiality of his diagnosis. Court found hospital liable for failure to take reasonable precautions to ensure his information was held confidential.
<i>Darling vs. Charleston Community Medical Hospital</i> (1965)	Case dismantled doctrine of charitable immunity. Court held that the governing board has the duty to establish mechanisms for the medical staff to evaluate, counsel, and when necessary, take action against an unreasonable risk of harm to a patient arising from the patient's treatment by a personal physician. Court held that, based on the hospital's obligation to select high-quality physicians to be medical staff members, the hospital may be held liable for a patient's injury caused by a physician who does not meet those standards but was given medical staff membership and privileges.
<i>Griswold vs. Connecticut</i> (1965)	Court ruled that the right to privacy limits governmental authority to regulate contraception, abortion, and other decisions affecting reproduction.
<i>Judge vs. Rockford Memorial Hospital</i> (1958)	Director of nurses wrote a letter to a nurse's professional registry stating that the hospital wanted to discontinue a particular nurse's services because narcotics were disappearing whenever the nurse was on duty. Court found communication to be privileged, because the director of nurses had a legal duty to make the communication in the interests of society. Nurse's claims for damages were denied by the court.
<i>Reisner vs. Regents of the University of California</i> (1995)	Physician failed to warn his patient that she had contracted HIV through a blood transfusion. As a result, the hospital and physician were sued when the patient's sexual partner was exposed to the virus. The court held that the hospital was liable for the physician's failure to warn.

(continues)

Table 3-5 Landmark Cases (continued)

Case	Court Decision
<i>Tarasoff vs. Board of Regents</i> (1976)	Determined that there was a duty to warn an individual against whom the patient has made a credible threat to harm.

- b. The U.S. Department of Health and Human Services (DHHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- c. The Privacy Rule standards address the use and disclosure of individuals' health information ("protected health information") by organizations subject to the Privacy Rule ("covered entities"), as well as standards for individuals' privacy rights to understand and control how their health information is used.
- d. Within DHHS, the Office for Civil Rights (OCR) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.
- e. See the Privacy Rule link in the references to view the entire rule.
- f. Goal of Privacy Rule
 - i. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care.
 - ii. HIPAA rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.
- g. Who is covered by the Privacy Rule
 - i. The Privacy Rule, as well as all the Administrative Simplification rules, applies to health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in electronic form in connection with transactions for which the Secretary of DHHS has adopted standards under HIPAA.
 - ii. Health plans: individual and group plans that provide or pay the cost of medical care are covered entities.
 - 1. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (HMOs), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies).
 - 2. Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans.
 - 3. Exceptions: a group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.
 - iii. Healthcare providers: every healthcare provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity.
 - iv. Healthcare clearinghouses: entities that process nonstandard information they receive from another entity into a standard, including billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

- v. Business associate defined: in general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
 - 1. Persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.
 - 2. A covered entity can be the business associate of another covered entity.
 - h. Which information is protected
 - i. Protected health information (PHI): the Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
 - ii. "Individually identifiable health information" is information, including demographic data, that relates to:
 - 1. The individual's past, present, or future physical or mental health or condition
 - 2. The provision of health care to the individual
 - 3. The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual
 - iii. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number).
 - iv. The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
 - v. De-identified health information. There are no restrictions on the use or disclosure of de-identified health information.
 - 1. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.
 - 2. There are two ways to de-identify information:
 - a. A formal determination by a qualified statistician
 - b. Removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.
- 7. Health Insurance Portability and Accountability Act (HIPAA) of 1996**
- a. Goals of HIPAA (see Figure 3-1)
 - i. Enacted to improve the portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes
 - ii. Addresses issues related to the portability of health insurance after leaving employment

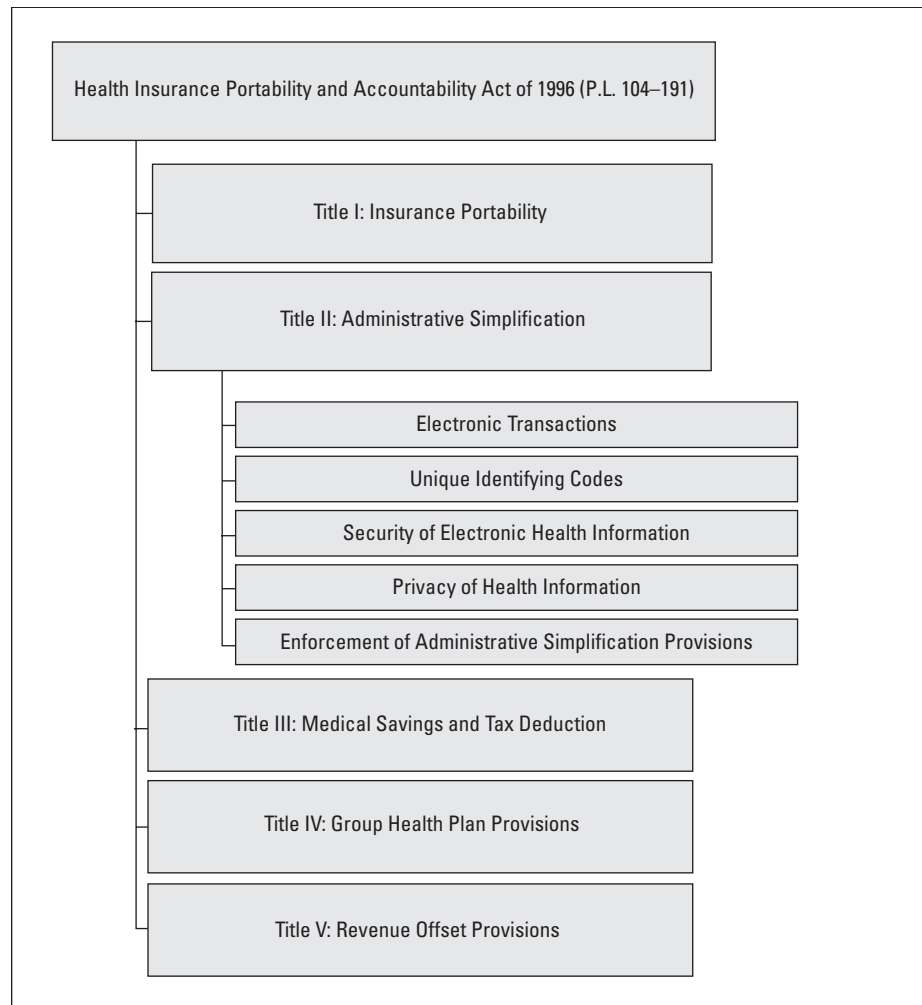


Figure 3-1 Five Portions of HIPAA

- iii. Created the Healthcare Integrity and Protection Data Bank (HIPDB), whose mission is to inform federal agencies about potential quality problems with clinicians, suppliers, and providers of healthcare services
- iv. Five portions of HIPAA
 - 1. Insurance portability
 - 2. Administrative simplification, including
 - a. Standardization of electronic formats for transmission of 11 specific electronic transactions
 - b. Unique identifying codes for healthcare providers, health plans, employers, and individuals
 - c. Security of electronic health information
 - d. Privacy of individually identifiable health information (Privacy Rule)
 - e. Enforcement of the administrative simplification provisions
 - 3. Medical savings and tax deductions
 - 4. Group health plan provision
 - 5. Revenue offset provisions

- b. Administration Simplifications**
 - i.** CMS is responsible for implementing various provisions of HIPAA.
 - ii.** Requires DHHS (which manages CMS) to improve the Medicare program under Title XVIII of the Social Security Act (SSA), the Medicaid program under Title XIX of the SSA, and the efficiency and effectiveness of the healthcare system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information
- c. Privacy Rule (2002)**
 - i.** HIPAA is first federal law that governs privacy of health information nationwide.
 - ii.** Prior to HIPAA Privacy Rule, there were no federal statutes or regulations of general application protecting the confidentiality of medical or personal information.
 - iii.** Ensures the protection of medical information shared with a covered entity, which are
 - 1.** Healthcare providers
 - 2.** Health plans
 - 3.** Healthcare clearinghouses
 - iv.** Privacy Rule restricts use and disclosure of personal health information and gives patients greater access to and protection of their medical records.
 - v.** Protects a patient's fundamental right to privacy and confidentiality; patients can expect
 - 1.** Privacy regarding their privileged communication
 - 2.** Security standards to ensure facilities, equipment, and patient information are safe from damage, loss, tampering, theft, or unauthorized access
 - vi.** Protected health information (PHI)
 - 1.** Personal health information given to a covered entity
 - 2.** Includes any information that is oral or is recorded on paper or electronically about a person's physical or mental health, services rendered, or payment for those services, and that includes personal information connecting the patient to the record
 - 3.** Examples of PHI
 - a.** Patient's name or address
 - b.** Social Security or other identification numbers
 - c.** Physician's personal notes
 - d.** Billing information
 - 4.** Authorization is required for the disclosure of PHI for purposes other than
 - a.** Treatment
 - i.** Covered entities may communicate freely with patients about treatment options and health-related information
 - b.** Payment
 - c.** Healthcare operations
 - 5.** Authorization is required to use PHI for
 - a.** Use or disclosure of psychotherapy notes
 - b.** Research purposes, unless a documented waiver is obtained from the institutional review board or privacy board
 - c.** Use and disclosure to third parties for marketing activities such as promoting services or selling lists of patients

- vii.** The HIPAA Privacy Rule does not include medical record retention requirements.
 - 1.** State laws generally govern how long medical records are to be retained.
 - 2.** The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other PHI for whatever period such information is maintained by a covered entity, including through disposal. See 45 CFR 164.530(c).
- d.** Security
 - i.** Under the Security Rule, covered entities, regardless of their size, are required, under § 164.312(a)(2)(i), to “assign a unique name and/or number for identifying and tracking user identity.”
 - 1.** A “user” is defined in § 164.304 as a “person or entity with authorized access.”
 - 2.** Accordingly, the Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that maintains electronic protected health information (e-PHI), so that system access and activity can be identified and tracked by user.
 - 3.** This pertains to workforce members within small or large healthcare provider offices, health plans, group health plans, and healthcare clearinghouses.
 - ii.** Encryption is a method of converting an original message of regular text into encoded text.
 - 1.** The text is encrypted by means of an algorithm (type of formula).
 - 2.** If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.
 - iii.** If covered entities allow employees to telecommute or work out of home-based offices and have access to e-PHI, they must implement appropriate safeguards to protect the organization’s data.
 - 1.** The automatic logoff implementation specification must be implemented if, after an assessment, the entity determines that the specification is a reasonable and appropriate safeguard in its environment.
 - iv.** Release of information form must include
 - 1.** A description of the information to be used or disclosed, written in clear language
 - 2.** Purpose of disclosure
 - 3.** Who will receive the information
 - 4.** Expiration date
 - 5.** Revocation
 - 6.** Statement that information released pursuant to authorization may be subject to redisclosure by the recipient and no longer protected
 - 7.** Signature of patient or legal representative
 - a.** If legal representative, then a description of his or her authority to act must be included on authorization form

- b. Consenting parties**
 - i. Minor:** generally defined as an individual who is under the age of majority.
 - 1.** Minors are unable to consent to their own care except in case of emancipated minor, medical emergencies, and certain identified health conditions.
 - 2.** Minors usually exercise their rights through a parent or other legal guardian.
 - ii. Emancipated minor:** a minor who has been awarded the status of adult due to situational changes such as marriage, pregnancy and other qualified situations
 - iii. Age of majority:** the legal recognition that an individual is considered responsible for, and has control over, his or actions.
 - 1.** The actions include consenting for health care, buying alcohol, getting married, enlisting in the armed forces, buying a house, and other actions.
 - 2.** Legal age is 18 in most states.
 - 3.** Age in Nebraska is 19, Mississippi is 21, and Nevada based age of majority upon graduating from high school.
 - iv. Competent adult:** an individual who is mentally capable and is above the age of majority.
 - v. Incompetent adult:** an individual who is no longer capable of controlling his or her action due to injury, illness, disability.
 - 1.** Exercises his or her rights through an appointed agent or guardian
- 8. Disclosed medical record may contain sensitive information (e.g., HIV/AIDS, drug/alcohol use, mental illness)**
- v. PHI can be used or disclosed without authorization but with patient agreement to**
 - 1.** Maintain a facility's patient directory
 - 2.** Inform family members or other identified persons involved in the patient's care or notify them on patient location, condition, or death
 - 3.** Inform appropriate agencies during disaster relief efforts
 - 4.** Public health activities related to disease prevention or control
 - 5.** Report victims of abuse, neglect, or domestic violence
 - 6.** Health oversight activities such as audits, legal investigations, licensure, or for certain law enforcement purposes or government functions
 - 7.** Coroners, medical examiners, funeral directors, or tissue/organ donations
 - 8.** Avert a serious threat to health and safety
 - 9.** In a bioterrorism threat or other public health emergency, HIPAA permits a covered entity to disclose PHI, without the patient's authorization, to public officials responding to the treat.
 - a.** The Privacy Rule recognizes that various agencies and public officials will need protected health information to deal effectively with a bioterrorism threat or emergency.

- b. To facilitate the communications that are essential to a quick and effective response to such events, the Privacy Rule permits a covered entity to disclose needed information to public officials in a variety of ways.
- 10. Revocation of authorization
 - a. The revocation must be in writing, and is not effective until the covered entity receives the written revocation.
 - b. A written revocation is not effective with respect to actions a covered entity took in reliance on a valid authorization, or where the authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself
- vi. Minimum necessary disclosure of PHI
 - 1. Covered entities must develop policies and practices to make sure the least amount of health information is shared.
 - 2. Employees must identify who regularly accesses PHI along with the types of PHI needed and the conditions for access.
 - 3. Does not apply to use or disclosure of medical records for treatment
- vii. Notice of privacy practices
 - 1. Patients have the right to adequate notice concerning the use or disclosure of their PHI on the first date of service delivery or as soon as possible after an emergency. New notices must be issued when the facility's privacy practices change.
 - 2. Notice of privacy practices must
 - a. Contain patient's rights and covered entities' legal duties
 - b. Be made available to patients in print
 - c. Be displayed at the site of service and posted on a website whenever possible
 - 3. Once a patient has received notice of his or her rights, covered entities must make an effort to get written acknowledgment of receipt of notice of privacy practices from the patient, or document reasons why it was not obtained, and copies must be kept of all notices and acknowledgments.
- viii. Privacy Rule grants patient rights over their PHI to include
 - 1. Receive notice of privacy practices at time of first delivery of service
 - 2. Request restricted use and disclosure, although the covered entity is not required to agree
 - 3. Have PHI communicated to them by alternate means and at alternate locations to protect confidentiality
 - 4. Inspect and amend PHI, and obtain copies, with some exceptions
 - 5. Request a history of disclosures for 6 years prior to the request
 - 6. Exceptions (disclosures for which an accounting is not required by covered entity) include disclosures
 - a. Made for treatment, payment, healthcare operations, or with prior authorization
 - b. To individuals of the PHI about themselves
 - c. For use in the facility's directory or to persons involved in the individual's care or other notification purposes
 - d. To meet national security or intelligence requirements

- e. To correctional institutions or law enforcement officials
 - f. That occurred before the compliance date for the covered entity
- 7. Contact designated persons regarding any privacy concern or breach of privacy within the facility or at DHHS
- ix. Rights of minors
 - 1. Parents have the right to access and control the PHI of their minor children, except when state law overrides parental control such as
 - a. HIV testing of minors without parental permission
 - b. Cases of abuse
 - c. When parents have agreed to give up control over their minor child
- x. Responsibility of healthcare institution
 - 1. Allow patients to see and copy their PHI
 - 2. Designate a full- or part-time privacy official responsible for implementing the programs
 - 3. Designate a contact person or office responsible for receiving complaints
 - 4. Develop a Notice of Privacy Practices document
 - 5. Develop policies and safeguards to protect PHI and limit incidental use or disclosure
 - 6. Institute employee training programs so everyone knows about the privacy policies and procedures for safeguarding PHI
 - 7. Institute a complaint process, and file and resolve formal complaints
 - 8. Make sure contracts with business associates comply with the Privacy Rule
- xi. HIPAA rules regarding psychotherapy notes
 - 1. Requires an authorization specifically allowing release of psychotherapy notes
 - 2. Defines psychotherapy notes as those taken by a mental health professional during a counseling session and kept separate from the rest of the medical record.
 - 3. Two key issues when determining which psychotherapy documentation is protected
 - a. Type of documentation
 - b. Where the records are kept
 - 4. Not all documentation by a mental health professional requires special protection—only the notes from a therapy session.
 - 5. Other documentation is handled in a similar manner to the rest of the medical record and includes prescriptions, medication monitoring, session start and stop times, modality and frequency of treatments, clinical test results, and summary items.
 - 6. When psychotherapy notes are maintained in another or with another record (e.g., medical record), they lose their special confidentiality protection
- xii. Violation of Privacy Rule (civil and criminal penalties)
 - 1. Civil penalty of \$100 up to a maximum of \$25,000 per year for each standard violated
 - 2. Criminal penalty for knowingly disclosing PHI is up to \$50,000 and 1 year in prison for obtaining or disclosing protected health information, up to \$100,000 and up to 5 years in prison for obtaining or disclosing PHI under false pretenses, and up to

\$250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm

8. Health Record Documentation

- a.** The record can serve and protect only when caregivers make a personal commitment to good medical record documentation.
- b.** The record should be complete, accurate, and legible to:
 - i.** Keep the healthcare team informed about patient progress
 - ii.** Enable caregivers to coordinate their efforts properly
 - iii.** Supply clinicians with data to evaluate and improve care
 - iv.** Ensure that timely decisions are made and communicated throughout the continuum of care
 - v.** Validate compliance with hundreds of requirements, including TJC accreditation standards and regulations established by federal, state, and local agencies
 - vi.** Furnish an objective basis for reimbursement by insurers
 - vii.** Provide a legal record of care rendered, thus defending against a malpractice claim
 - viii.** Furnish data to conduct research and clinical trials
- c.** Patient record is used to:
 - i.** Establish duty
 - ii.** Determine if standards of care were met
 - iii.** Evaluate damages
 - iv.** Fix cause
- d.** Departures from appropriate recordkeeping are used by the plaintiff's attorney to create the impression that care itself was negligent. These include:
 - i.** Alterations of entries without proper identification
 - ii.** Feuding among caregivers
 - iii.** Illegibility of written notes and orders
 - iv.** Late entries
 - v.** Missing data or test results
 - vi.** Omission of information
 - vii.** Time gaps
- e.** Documentation Guidelines for Entries
 - i.** Entries should be complete, accurate, legible, timed, and signed by the author, using full name and credentials.
 - ii.** Entries should be made on or about the time of treatment.
 - iii.** Made on approved forms and filed by order of the chart
 - iv.** Made in the appropriate sequence in the record, avoiding gaps with previous entries and lapses in time
 - v.** Late entries should be clearly marked as such.
 - vi.** Entries by students, interns, and residents should be countersigned.
 - vii.** Only approved abbreviations and terminology should be used.
 - viii.** Corrections, addenda, and changes to entries should be done according to policy.
 - ix.** Adverse episodes and subsequent interventions should be written objectively.

9. Health Records in Court


- a.** Definitions Relevant to Court Procedure
 - i.** Appeal: the process by which a decision of a lower court is brought for review to a court of higher jurisdiction, typically known as an appellate court

- ii. Court order: a written command or direction ordered by a court or judge
- iii. Cross examination: questioning of a witness by the opposing attorney
- iv. Defendant: the party against whom a complaint is brought
- v. Direct examination: initial questioning of a witness by the attorney who has requested the witness to testify
- vi. Jurisdiction: the power of authority which each court has to hear cases; a court's jurisdiction is determined by the subject matter of the case, the persons in the case, and by geographical area
- vii. Legal precedent: refers to a previous case decision that serves as an authority in identical or similar cases
- viii. Memorandum of law: a document prepared by an attorney, prior to trial, which outlines the case and notes past decisions that support the client's position; usually submitted to the court for reference
- ix. Motions: requests to the court made by plaintiff's or defendant's attorney
- x. Plaintiff: the party who brings a complaint against another
- xi. Pleadings: statements of complaint by plaintiff, answer from defendant, and possibly a counterclaim by defendant
- xii. Pretrial discovery: procedures whereby the attorneys for opposing sides in a case find out what information the opposing side possesses
- xiii. Re-cross examination: second series of questions directed to a witness by the opposing attorney; takes place following redirect examination
- xiv. Redirect examination: second series of questions directed to a witness by the attorney who had originally requested the witness to testify
- xv. Res gestae: "things done," which means that hearsay statements made during an incident are admissible as evidence
- xvi. Res ipsa loquitur: "The thing speaks for itself," which means that something is self-evident (e.g., erroneous surgical removal of healthy limb while leaving unhealthy limb)
- xvii. Res judicata: "The thing is decided," which means the final judgment of a competent court is conclusive
- xviii. Respondeat superior: "Let the master answer," which means that an employer is responsible for the legal consequences of an employee's actions
- xix. Stare decisis: the doctrine that states that court decisions should be regarded as precedents for guidance in subsequent cases involving the same legal issues
- xx. Summation: statement made by an attorney at the closing of a trial, summarizing the client's case
- xxi. Summons: a court order notifying the defendant of a civil suit, and the date and place the defendant must appear to answer the complaint
- xxii. Tort: An injury of wrong committed against an individual or his or her property.
 - 1. Types of torts (intentional and unintentional)
 - a. Malpractice
 - b. Negligence

- c.** Intentional torts (assault and battery)
 - d.** False imprisonment
 - e.** Defamation: oral (slander), written (libel)
 - f.** Invasion of privacy
 - g.** Fraud/intentional misrepresentation
 - h.** Inflicting of emotional or mental distress
 - xxiii.** Venue: the particular geographical area in which an action or prosecution may be brought to trial
 - xxiv.** Voir dire: a preliminary examination to determine the competency of a witness or juror
 - b.** Evidence
 - i.** Information that may be considered in the determination of a controversy taking place in a court of law
 - ii.** The means, sanctioned by law, of ascertaining the truth respecting a question of fact in a judicial proceeding
 - iii.** Best-evidence rule
 - 1.** Original documents must be produced in a legal proceeding.
 - 2.** Microfilm or other media reproductions are acceptable if the original record has been destroyed.
 - iv.** Types of evidence
 - 1.** Direct: obtained from testimony of witnesses who possess actual knowledge of the facts of the case
 - a.** Whistleblower: raises concerns to external agency
 - 2.** Indirect or circumstantial: facts that furnish reasonable ground for inferring the existence of some other connected facts
 - 3.** Real or demonstrative: objects, documents, or anything that can be seen
 - 4.** Hearsay
 - a.** Evidence based on someone else's knowledge and observations, not on that of the witness
 - b.** Health records are hearsay evidence.
 - c.** Even though health records are hearsay, they may be entered into court as evidence in exception to hearsay rules because they are business records, which are admissible into court as evidence.
 - v.** Admissibility
 - 1.** Evidence that may be properly introduced in a legal proceeding
 - 2.** The determination as to admissibility is based on legal rules of evidence and is made by the trial judge or a screening panel.
 - 3.** For medical records to be admissible, they must meet the following criteria:
 - a.** Applicable to the business record rule
 - b.** The court must be confident that the information contained in the record is complete, accurate, and timely.
 - c.** The court must accept that the information was recorded as the result of treatment, not in anticipation of a legal proceeding.
 - 4.** Discoverability
 - a.** Quality improvement, peer review, and incident reports are not discoverable in some states.
 - 5.** Business record rule
 - a.** Records made and kept in the regular course of business may be entered into court as evidence.
 - b.** Medical records are business records.

6. Testifying about admissibility
 - a. Typically, the health record custodian is called upon to authenticate records by providing testimony about the process or system that produced the records.
 - i. An organization's recordkeeping program should consist of policies, procedures, and methods that support the creation and maintenance of reliable, accurate records.
 - ii. If so, the records will be admissible into evidence.
 - b. Electronic and imaged health records
 - i. Case law and the Federal Rules of Evidence provide support to allow the output of an EHR system to be admissible in court.
 - ii. "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."
- vi. Legal proceedings
 1. Filing a civil suit
 - a. Civil action is known by names of plaintiff and defendant, with plaintiff name listed first.
 - b. Plaintiff's attorney pays fee and files a complaint or petition with clerk of the proper court to formally begin legal proceeding.
 - c. Complaint states the facts on which the action is based, damages alleged, and the judgment or relief being sought.
 2. Civil pretrial procedure (see Table 3-6)
 - a. Complaint
 - i. Made by plaintiff
 1. Initial pleading in a lawsuit
 2. Plaintiff alleges a cause of action.
 3. Plaintiff request for wrong to be remedied by the court
 - b. Answers to complaint by defendant
 - c. Motions requesting court to make a variety of rulings
 - d. Pretrial discovery
 - i. Facilitates out-of-court settlements
 - ii. Disclosure of facts and documents by one party at the request of the other

Table 3-6 Civil Pretrial Procedure

Complaint	
Answers	
Motions	
Pretrial discovery	
Notice of trial	
Memorandum of law	

- iii. Obtained through depositions and interrogatories that are used to prepare the case for trial
 - 1. Deposition
 - a. Sworn statement of fact
 - b. Made outside of court
 - c. May be admitted as evidence in court
 - 2. Interrogatories
 - a. Written questions presented to a party or witness
 - b. Designed to gather information to assist parties prepare for trial
 - e. Notice of trial: a trial date is set.
 - f. Memorandum of law: a case description may be written by attorneys for both sides.
 - 3. Civil trial process
 - a. Jury selection
 - b. Opening statements by plaintiff's and defendant's attorneys
 - c. Presentation of the plaintiff's case
 - d. Presentation of defendant's case
 - e. Plaintiff's rebuttal
 - f. Answer to plaintiff's rebuttal
 - g. Closing arguments
 - h. Instructions to jury by judge
 - i. Verdict read
 - j. Judgment and execution for remedy or damages to be assessed
 - k. Appeal by disappointed party if judge refuses to grant a post-trial motion for a new trial
 - c. Health Information Practitioner's Proper Conduct as a Witness
 - i. Review record and deposition prior to testimony
 - ii. Make a copy of the record and paginate prior to taking to court
 - iii. Take original record and copy to court
 - iv. Request to submit copy of record in lieu of original into court as evidence
 - v. Witness may refer to health record to refresh recollection.
 - vi. Dress conservatively
 - vii. Be polite, sincere, courteous
 - viii. Organize thoughts
 - ix. Use simple and succinct terminology
 - x. Pay attention to objections
 - xi. Do not answer questions if not qualified to answer
 - xii. Return original record to health care facility for proper storage
- 10. Negligence and Malpractice**
- a. Principles of Liability
 - i. Before an individual can bring a lawsuit to establish some form of liability (malpractice, negligence) against a healthcare provider, the individual must have established a relationship with that provider.
 - 1. Types of relationships
 - a. Physician/patient
 - b. Hospital/patient
 - c. Hospital/physician
 - b. Negligence
 - i. Results when a person does not act the way a reasonably prudent person would act under the same circumstances

- ii. Results from a person committing an act, or failure to act as a reasonably prudent person would act in the given circumstance
- iii. When negligence results in patient injury, malpractice can be said to have occurred.
- iv. Careless conduct that is outside the generally accepted standard of care
 - 1. Standard of care
 - a. What an individual is expected to do or not do in a given situation
 - b. Established by professional associations, statute or regulation, or by practice
 - c. Considered to represent expected behavior unless a court finds differently
- v. Negligence categorized
 - 1. Malfeasance: execution of an unlawful or improper act
 - 2. Misfeasance: improper performance of an act
 - 3. Malpractice
 - a. Negligence or carelessness of a professional person such as a physician
 - b. Patient injury or death due to negligence caused by a professional person such as a nurse, pharmacist, or physician
 - 4. Criminal negligence: reckless disregard for the safety of another; the willful indifference to an injury that could follow an act
- vi. Four components must be present for plaintiff to recover damages caused by negligence.
 - 1. Duty: a treatment or service owed to a patient (e.g., duty to give the right medication to the right patient)
 - 2. Breach: failure to perform to the applicable standard of care (e.g., nurse gave patient wrong medication)
 - 3. Cause: breach of duty, causing the resulting injury (e.g., patient suffered hallucinations, resulting in her getting out of bed without help and falling)
 - 4. Damage: patient injured (e.g., when she fell, she broke her hip)
 - a. Three types
 - i. Nominal: awarded for the vindication of a right in which minimal injury can be proved
 - ii. Actual: compensatory damages are awarded to “make the plaintiff whole.”
 - iii. Punitive: exemplary damages are awarded above and beyond actual damages when there is proof of outrageous, malicious, or intentional conduct.

Duty of Care + Breach of Duty of Care + Causation + Damages = **Negligence**

- vii. Statute of limitations: legislatively imposed time constraints that restrict the period of time after the occurrence of an injury during which a legal action must be commenced
- viii. Tort: an action brought when party believes that another party caused harm through wrongful conduct and seeks compensation for that harm

- 1. Three categories of tort liability**
 - a. Negligent**
 - i.** When a person does not act the way a reasonably prudent person would act under the same circumstance
 - ii.** Care rendered is outside the generally accepted standard of care.
 - b. Intentional**
 - i.** The person committed an act knowing that harm would likely occur.
 - ii. Assault and battery**
 - 1.** The individual does not give permission or authority for an act.
 - 2.** Assault occurs when an individual is placed in reasonable anticipation of being touched in a way that is insulting, provoking, or will cause the individual physical harm.
 - 3.** Battery consists of physical contact involving injury or offense.
 - iii. Defamation of character**
 - 1.** A communication about someone to another person that tends to injure the former person's reputation
 - 2.** Slander: spoken character defamation
 - 3.** Libel: written character defamation
 - iv.** False imprisonment: a healthcare provider's effort to prevent a patient from leaving a hospital when the patient insists on leaving (does not include mental illness or persons with contagious diseases)
 - v.** Fraud: a willful and intended misrepresentation that could cause harm or loss to a person or property
 - vi.** Invasion of privacy: negligent disregard for patient right of privacy
 - vii.** Willful infliction of mental distress: includes mental suffering resulting from such things as despair, shame, grief, and public humiliation
 - c. Liability without fault: property liability, wherein a manufacturer, seller, or supplier of equipment or supplies is liable to one with whom there is no contractual relationship and who suffers harm from the equipment or supplies**
- ix. Assumption of risk**
 - 1.** A method used to limit liability either completely or in part
 - 2.** A plaintiff who voluntarily exposes himself to a known and appreciated danger may not recover damages caused by incurring that risk.
- x. Breach of contract: involves express contracts and the failure to perform these contracts**
- xi. Defamation**
 - 1.** Wrongful injuring of another person's reputation
 - 2.** May expose the person to ridicule, contempt, or hatred and tends to diminish the esteem, respect, goodwill, or confidence in which the person is held
- xii. Failure to warn: also referred to as failure to protect; a negligence theory that applies to a psychiatrist's failure to take steps to protect an innocent third party from a dangerous patient**

- xiii.** Good Samaritan statutes
 - 1. These statutes protect physicians and other rescuers from civil liability as a result of their acts or omissions in rendering emergency care.
 - 2. If, however, the rescuer acts in a willful, wanton, or reckless manner in providing emergency treatment, he or she cannot avail himself of the Good Samaritan statute as a defense.
- xiv.** Invasion of privacy: the dissemination of information about another person's private, personal matters
- xv.** Libel: defamation expressed in writing, pictures, or signs
- xvi.** Medical abandonment: unilateral severing, by the physician, of the physician–patient relationship without giving the patient reasonable notice, at a time when there is a necessity for continuing care
- xvii.** *Repondeat superior*
 - 1. “Let the superior respond” reflects the idea that the superior is responsible for the actions of the superior's employee or agent.
 - 2. Also referred to as vicarious liability
 - 3. Healthcare organization, such as hospital, is responsible for the negligent acts of its employees committed within the course and scope of their employment.
- xviii.** *Res ipsa loquitur*: “the thing speaks for itself”
 - 1. Injury would not ordinarily occur without someone's negligence.
 - 2. The medical professional had exclusive control and management over the instrument or cause of the accident.
 - 3. The injury could not have occurred as a result of any action by the patient.
- xix.** Slander: defamation expressed orally or with transitory gestures
- xx.** Statute of limitation: a law that sets forth a fixed time period in which a lawsuit must be brought

11. Computer-Based Health Records

- a.** Computer-Based Records as Evidence
 - i. Courts have developed standards for establishing the trustworthiness of computerized records.
- b.** Security
 - i. Procedures must be in place to protect information from sabotage, hackers, and viruses.
 - ii. Use passwords and other authorization devices that are changed at regular intervals
 - iii. Access control that can limit who is able to view, enter, edit data, or print various sections of the record
 - iv. Controls that prevent tampering with, changing, or editing of existing entries
 - v. Audit trails that can locate sources of attempts at unauthorized access
 - vi. Limitations on printouts of record
 - vii. Automatic log-off protocols when terminal is unused for a period of time
 - viii. Limited access to patient records by employees on a need-to-know basis
 - ix. Encryption codes that prevent stored or transmitted data from being intercepted by unauthorized individuals

12. Ethical Issues for Health Information Practitioners

a. Ethics

- i.** A process of reasoned discourse among decision makers
- ii.** Decision makers must carefully consider the shared and competing values and ethical principles that are important to the decision to be made.

b. Ethical decision making requires everyone to consider the perspectives of others.

c. Ethical decision making demonstrates respect for others and recognizes the importance of doing good, respecting others, not harming others, and treating people fairly.

d. Core Ethical Responsibilities of Health Information Practitioner

- i.** Maintain an accurate and timely patient database
- ii.** Be honest and respectful toward patients, peers, and public
- iii.** Protect the privacy of all patients
- iv.** Demonstrate compassion to patients and peers
- v.** Design forms to ensure that patients understand what they are signing
- vi.** Coding for research and reimbursement, and coding accurately, to avoid fraud and abuse violations
- vii.** Designing and implementing the health information system to ensure completeness, accuracy, and timeliness of documentation
- viii.** Releasing patient information with special attention to, and protections assigned for, genetic, adoption, drug and alcohol treatment, sexual and behavioral issues
- ix.** Complying with regulations and standards from many sources, including the government, accreditation and licensure organizations, and the healthcare facility
- x.** Reporting quality review outcomes honestly and accurately
- xi.** Ensuring that research and decisions supporting activities are accurate and reliable
- xii.** Releasing accurate information for public health purposes for patients with communicable diseases
- xiii.** Supporting managers, by providing accurate reliable information about patients, providers, and patterns of care
- xiv.** Ensuring that the patient record (paper-based and electronic formats) meets the standards of privacy and security
- xv.** Participating in activities to ensure that the needs of the healthcare facility are met and not jeopardized
- xvi.** Serve as an advocate for the patient, healthcare team, and community
- xvii.** Work in the emerging e-health system to ensure that high-quality information is provided to patients and that patient privacy is protected
- xviii.** Comply with all laws, regulations, and policies that govern health information management
- xix.** Ensure the privacy, confidentiality, and security of patient information and report violators to the proper authorities
- xx.** Uphold the AHIMA codes of ethical standards

e. Obligations to Employer

- i.** Demonstrate loyalty to the employer
- ii.** Protect committee deliberations
- iii.** Comply with all laws, regulations, and policies that govern the health information system
- iv.** Recognize both authority and the power associated with the job responsibility

- f. Obligations to Public
 - i. Advocate change when patterns or system problems are not in the best interests of the patients
 - ii. Refuse to participate in or conceal unethical practices
 - iii. Report violations of practice standards to the proper authorities
- 13. Freedom of Information Act**
 - a. Requires that records pertaining to the executive branch of the federal government be available to the public except for matters that fall within exempted areas
 - b. Exempted matter is considered to be unwarranted invasion of privacy
 - c. To meet the test of being an “unwarranted invasion of privacy,” the following conditions must exist:
 - i. The information must be contained in a medical, personnel, or a similar file.
 - ii. Disclosure of the information must constitute an invasion of privacy.
 - iii. The severity of such invasion must outweigh the public interest in disclosure.
- 14. Minimum Necessary Standard**
 - a. Just because a person works in a healthcare facility, he or she does not have a blanket access to all patient information.
 - b. Only the minimum amount of information necessary to fulfill the purpose of the request should be shared with internal users and external requestors.
 - c. The minimum necessary standard does not apply in the following situations:
 - i. Use or disclosure for treatment purpose
 - ii. When patient has specifically authorized the release of more information
 - iii. Disclosure pursuant to applicable law
- 15. Patient Protection and Affordable Care Act (PPACA)**
 - a. PPACA, commonly called Obamacare or Affordable Care Act (ACA), is U.S. federal legislation signed into law by President Barack Obama on March 23, 2010. Together with the Health Care and Education Reconciliation Act, it represents the most significant government expansion and regulatory overhaul of the U.S. health system since the passage of Medicare and Medicaid in 1965.
 - b. ACA is aimed at increasing the affordability and rate of health insurance coverage for Americans and reducing the overall costs of health care (for individuals and the government). It provides a number of mechanisms—including mandates, subsidies, and tax credits—to employers and individuals to increase the coverage rate and health insurance affordability.
 - c. ACA requires insurance companies to cover all applicants within new minimum standards, and offer the same rate regardless of preexisting condition or sex. Additionally, these reforms are designed to improve healthcare outcomes and streamline the delivery of health care.
 - d. Congressional Budget Office projects that ACA will lower both future deficit and Medicare spending.
- 16. Amendment to HIPAA Privacy, Security, Breach Notification, and Enforcement Rules**
 - a. On January 17, 2013, DHHS’s Office for Civil Rights (OCR) issued the long-anticipated final omnibus amendments (“2013 Amendments”) to the Privacy, Security, Breach Notification and Enforcement Rules

(“HIPAA Rules”), as directed pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

- b. The 2013 Amendments were effective as of March 26, 2013, and compliance with applicable requirements generally must have been made within 180 days, by September 23, 2013 (with important exceptions for existing business associate arrangements).
- c. Significant penalties apply for noncompliance.

Houston Honorary Hospital Authorization for Release of Information			
Name: _____		Medical Record #: _____	
Address: _____		Phone: _____	
Social Security #: _____		Date of Birth: _____	
<i>I authorize Houston Honorary Hospital to release my medical record information to the following person, facility, or agency:</i>			
Name: _____		Attention: _____	Phone: _____
Street: _____		City/Town: _____	State: ____ Zip: _____
<i>The person filling out this form must provide details as to date(s) of requested information. Please note that a request for release of psychotherapy notes cannot be combined with any other type of request. Specify information to be released, e.g., Entire Record, Admission(s) Documentation, Discharge Summary(ies), Transfer Summary(ies), Evaluations, Assessments and Tests, Consultation(s) including names of consultant(s), Treatment Plan(s), ISP(s) & PSTP(s), Physical Exam & Lab Reports, Progress Note(s):</i>			

Purpose for the authorization: <input type="checkbox"/> The subject of the information or Personal Representative initiated the authorization (specific purpose not required) or <input type="checkbox"/> Continuity of care <input type="checkbox"/> Facilitate billing <input type="checkbox"/> Referral <input type="checkbox"/> Obtain insurance, financial or other benefits <input type="checkbox"/> Other purpose (please specify): _____			

Figure 3-2 Sample Release of Information Form

Houston Honorary Hospital Authorization for Release of Information (<i>continued</i>)	
<p>I understand that I have a right to revoke this authorization at any time. If I revoke this authorization, I must do so in writing and present it to the person at Houston Honorary Hospital. I understand that the revocation will not apply to information that has already been released pursuant to this authorization. This authorization will expire in 12 months unless otherwise specified (specify a date, time period or an event): _____.</p> <p>_____. I understand that once the above information is disclosed it may be redisclosed and no longer protected by federal or state privacy laws or regulations. I understand that authorizing the use or disclosure of the information identified above is voluntary. I need not sign this form to receive treatment or services from Houston Honorary Hospital. However, lack of ability to share or obtain information may prevent Houston Honorary Hospital, and/or other person, facility, or agency, from providing appropriate and necessary care.</p>	
<p>_____ Your signature or Personal Representative's signature</p>	<p>_____ Date</p>
<p>_____ Print name of signer</p>	
<p>THE FOLLOWING INFORMATION IS NEEDED IF SIGNED BY A PERSONAL REPRESENTATIVE</p>	
<p>Type of authority (e.g., court appointed, custodial parent) _____</p>	
<p>Specially Authorized Releases of Information (please initial all that apply)</p>	
<p>____ To the extent that my medical record contains information concerning alcohol or drug treatment that is protected by Federal Regulation 42 CFR, Part 2, I specifically authorize release of such information.</p>	
<p>____ To the extent that my medical record contains information concerning HIV antibody and antigen testing that is protected by MGL c.111 §70F, or an HIV/AIDS diagnosis or treatment, I specifically authorize disclosure of such information.</p>	
<p>_____ Your signature or Personal Representative's signature</p>	<p>_____ Date</p>
<p>INSTRUCTIONS:</p>	
<p>1. This form must be completed in full to be considered valid.</p>	
<p>2. Distribution of copies: original to appropriate medical record; copy to individual or Personal Representative.</p>	
<p>Houston Honorary Hospital Form Authorization for Release of Information Page 2 of 2 HIPAA-F-7 (4/22/xx)</p>	

Figure 3-2 Sample Release of Information Form (*continued*)

§ THE STATE OF TEXAS

§ IN THE MATTER OF A

§ COUNTY OF COWBOYS

§ GRAND INVESTIGATION

TO THE SHERIFF OR ANY OTHER PEACE OFFICER

GREETINGS

WHEREAS the grand jury of Cowboys County is inquiring into certain offenses liable to indictment; and

WHEREAS Article 20.10 of the Texas Code of Criminal procedure provides that the attorney representing the state, in term time or in vacation may issue a summons or an attachment for any witness in the county, which summons or attachment may require the said witness to appear before the grand jury at a time fixed, or forthwith, without stating the matter under investigation; and

WHEREAS any Texas peace officer receiving this process shall execute the same forthwith by reading the same in the hearing of the said witness or by delivering a copy of this showing the time and manner of service, if served, and if not served, said officer shall show in his return the cause of his failure to serve it; and if the witness could not be found, he shall state the diligence he has used to find him, and what information he has as to the whereabouts of the witness;

NOW THEREFORE YOU ARE HEREBY COMMANDED to forthwith summon, the custodian of records, John Doe, Houston Honorary Hospital to appear before the 401st Judicial District Court Grand Jury for August Term, 20xx at 403 Tyson Street, 1st floor, Cowboy, Texas at 10 am on September 20, 20xx.

FURTHER, you are directed that the said witness shall bring with him the following writing or other thing desired as evidence in accordance with Article 24.02 of the Texas Code of Criminal procedure, and more specifically described as follows:

PRODUCE TRUE AND CORRECT COPIES OF MEDICAL RECORD ON JOHN DOE; DATE OF BIRTH December 25, 20xx.

Figure 3-3 Sample Subpoena Duces Tecum

<p>§ IN THE DISTRICT COURT OF</p> <p>§</p> <p>§ COWBOYS COUNTY, TEXAS</p> <p>§</p> <p>§ 1051st JUDICIAL DISTRICT</p> <p>DIRECT QUESTIONS TO BE PROPOUNDED TO THE WITNESS, CUSTODIAN OF MEDICAL RECORDS FOR Houston Honorary Hospital</p> <ol style="list-style-type: none"> 1. Please state your name and occupation. 2. Have you been served with a subpoena duces tecum for the production of medical records for John Doe? 3. Please state whether you have in your custody or subject to your control the records pertaining to John Doe. 4. Please hand the Notary Public propounding these questions a complete copy of all such records, reports, etc., described in the subpoena pertaining to Doe. 5. Are the records you have furnished the Notary Public in response to Question Number 4 a complete and accurate copy of the records described in the subpoena that you have on this individual? 6. Were records not produced that have been destroyed or purged? 7. Were these records kept in your regular course of business? 8. Is it in the regular course of your business, or of an employee in your office having personal knowledge of the acts recorded, to prepare the records or transmit the information included in the records of John Doe? 9. Were the records made at or near the time of the performance of the act recorded therein or reasonably soon thereafter? 10. Does the source of the information, and the method and circumstance of its preparation, establish the trustworthiness of the records, notes, and or reports? <p>_____ Signature of Custodian</p> <p>BEFORE ME, THE UNDERSIGNED AUTHORITY on this day personally appeared _____, custodian of Medical Records for Houston Honorary Hospital known to me to be the person whose name is subscribed to the foregoing instrument in the capacity therein stated, and acknowledged to me that the answers to the foregoing questions are true as stated. I further certify that the records attached hereto are exact duplicates of the original records.</p> <p>GIVEN UNDER MY HAND AND SEAL OF OFFICE, this the _____ day of _____ year of 20xx.</p> <p>_____ Notary Public in and for the State of Texas</p> <p>My commission expires _____</p>
<p>Figure 3-4 Sample Deposition</p>

STATE OF TEXAS	§ IN THE _____
Vs.	§ COURT IN AND FOR
_____	§ COWBOYS COUNTY, TEXAS

AFFIDAVIT

Before me, the undersigned authority, personally appeared _____,
who, being by me duly sworn, deposed as follows:

My name is _____, I am of sound mind, capable of making
this affidavit, and personally acquainted with the facts herein stated:

I am the Custodian of the records of _____. Attached hereto
are _____ pages of records from _____. These said _____ pages of
records are kept by **Houston Honorary Hospital** in the regular course of business, at
it was the regular course of business of **Houston Honorary Hospital**, for an employee
or representative of **Houston Honorary Hospital**, with knowledge of the act, event,
condition, opinion, or diagnosis, recorded to make the record or transmit information
thereof to be included in such record; and the record was made at or near the time
or reasonably soon thereafter. The records attached hereto are the original or exact
duplicates of the original.

Affiant

SWORN TO AND SUBSCRIBED before me the _____ day of _____ of the
_____ year.

Notary Public
State of Texas

My commission expires _____

Figure 3-5 Sample Affidavit

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please read it carefully.

Introduction to Privacy

We are required by law to maintain the privacy of your medical information. We are also required to give you this Notice about our privacy practices, our legal duties, and your rights concerning your medical information. We must follow the privacy practices that are described in this Notice while it is in effect. We reserve the right to change our privacy practices and the terms of this Notice at any time, provided such changes are permitted by law. We reserve the right to make the changes in our privacy practices and the new terms of our Notice effective for all medical information that we maintain, including medical information we created or received before we made the changes. If we make a significant change in our privacy practices, we will amend this Notice and make the new Notice available upon request.

You may request a copy of our Notice at any time. For more information about our privacy practices, or for additional copies of this Notice, please contact _____.

Joint Notice of Privacy

This Joint Notice applies to the privacy practices of **Houston Honorary Hospital** for the sole purpose of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HIPAA Privacy Rules and with the Texas Medical Privacy Act, Texas Health & Safety Code § 181.

Uses and Disclosures of Medical Information

We use and disclose medical information about you for treatment, payment, and healthcare operations.

Treatment: We may use and disclose your medical information to a physician or other healthcare provider to provide treatment to you. This includes coordination of your care with other healthcare providers, and with health plans, consultation with other providers, and referral to other providers related to your care.

Payment: We may use and disclose your medical information to obtain payment for services we provide to you. Payment includes submitting claims to health plans and other insurers, justifying our charges for and demonstrating the medical necessity of the care we deliver to you, determining your eligibility for health plan benefits for the care we furnish to you, obtaining precertification or preauthorization for your treatment or referral to other healthcare providers, participating in utilization review of the services we provide to you and the like. We may disclose your medical information to another healthcare provider or entity subject to the federal Privacy Rules so they can obtain payment.

Healthcare Operations: We may use and disclose your medical information in connection with our healthcare operations. Healthcare operations include:

- Quality assessment and improvement activities
- Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider accreditation, certification, licensing or credentialing activities
- Medical review
- Legal services and auditing, including fraud and abuse detection and compliance
- Business planning and development

(continues)

Figure 3-6 Sample Notice of Privacy Practices

- Business management and general administrative activities, including management activities relating to privacy, customer service, resolution of internal grievances, and creating de-identified medical information or a limited data set

We may disclose your medical information to another provider or health plan that is subject to the Privacy Rules, as long as that provider or plan has a relationship with you and the medical information is for their healthcare quality assessment and improvement activities, competence and qualification evaluation and review activities, or fraud and abuse detection and prevention.

On Your Authorization: You may give us written authorization to use your medical information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Unless you give us a written authorization, we cannot use or disclose your medical information for any reason except those described in this Notice.

To Your Family and Friends: We may disclose your medical information to a family member, friend, or other person to the extent necessary to help with your health care or with payment for your health care. We may use or disclose your name, hospital location, and general condition or death to notify, or assist in the notification of (including identifying or locating) a person involved in your care. We may also disclose your medical information to whomever you give us permission. Before we disclose your medical information to a person involved in your health care or payment for your health care, we will provide you with an opportunity to object to such uses or disclosures. If you are not present, or in the event of your incapacity or an emergency, we will disclose your medical information based on our professional judgment of whether the disclosure would be in your best interest. We will also use our professional judgment and our experience with common practice to allow a person to pick up filled prescriptions, medical supplies, or other similar forms of medical information.

Facility Directory: We may use your name, your location, your general medical condition, and your religious affiliation in our facility directories. We will disclose this information to members of the clergy and, except for religious affiliation, to other persons who ask for you by name. We will provide you with an opportunity to restrict or prohibit some or all disclosures for facility directories unless emergency circumstances prevent your opportunity to object.

Disaster Relief: We may use or disclose your medical information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

Health-Related Services: We may use your medical information to contact you with information about health-related benefits and services or about treatment alternatives that may be of interest to you. We may disclose your medical information to a business associate to assist us in these activities.

Business Associate: We may disclose your medical information to a company or individual performing functions or activities to or on our behalf.

Marketing: We will not use your medical information for marketing purposes without your authorization. **Houston Honorary Hospital** uses commercially purchased lists. We must obtain your authorization for all marketing purposes except for face-to-face conversations about services and treatment alternatives. You may also receive information through a membership program that you have joined. If you have opted in or have joined a membership program and you no longer wish to receive further

Figure 3-6 Sample Notice of Privacy Practices (continued)

information, please indicate this in writing by completing a marketing opt-out form, which you may get by calling 777-777-7777.

Fundraising: We may use your demographic information and the dates of your health care to contact you for our fundraising purposes. We may disclose this information to a business associate or foundation to assist us in our fundraising activities. If you would like more information on the **Houston Honorary Hospital Foundation** or a description of how you may opt out of receiving future fundraising communications, please indicate this in writing by calling 777-777-7777 and requesting an opt-out form.

Public Benefit: We may use or disclose your medical information as authorized by law for the following purposes deemed to be in the public interest or benefit:

- Public health activities including disease and vital statistics reporting, child abuse reporting, adult protective services, and FDA oversight
- Employers, regarding work-related illness or injury
- Cancer registry
- Trauma registry
- Birth registry
- Health oversight agencies
- In response to court and administrative orders and other lawful processes
- To law enforcement officials pursuant to subpoenas and other lawful processes, concerning crime victims, suspicious deaths, crimes on our premises, reporting crimes in emergencies, and for purposes of identifying or locating a suspect or other person
- To coroners, medical examiners, and funeral directors
- To organ procurement organizations
- To avert a serious threat to health or safety
- In connection with certain research activities
- To correctional institutions regarding inmates
- As authorized by state worker's compensation laws
- To the military, to federal officials for lawful intelligence, counterintelligence, and national security activities, and to correctional institutions and law enforcement regarding persons in lawful custody

Individual Rights

You have the right to review or receive a copy of your medical information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot practicably do so. You must make a request in writing to obtain access to your medical information. You may obtain a form to request access or a copy of your medical information from the Release of Information department located at the facility where you obtain your medical care. There is a charge for a copy of your medical information.

Accounting of Disclosures

You have the right to receive an accounting of all uses and disclosures of your health information that was not authorized by you and that was not used by **Houston Honorary Hospital** for the sole purposes of treatment, payment, and health care operations. You must request this accounting in writing. This accounting is maintained for a period of 6 years beginning on April 14, 20xx, the effective date of this Notice. You may obtain a form to request an accounting of disclosures from the Release of Information department located at the facility where you obtained your medical care. *(continues)*

Figure 3-6 Sample Notice of Privacy Practices (continued)

Restrictions: You have the right to request that we place additional restrictions on our use or disclosure of your medical information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency). You must make this request in writing.

Confidential Communications: You have the right to request that we communicate with you about your medical information by alternative means or to alternative locations. You must make your request in writing. We must accommodate your request if: it is reasonable; specifies the alternative means or location; and provides a satisfactory explanation of how payments will be handled under the alternative means or location you request.

Amendment: You have the right to request that we amend your medical information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended and the originator remains available or for certain other reasons. If we deny your request, we will provide you a written explanation. You may respond with a statement or disagreement to be appended to the information you want amended. If we accept your request to amend the information, we will make reasonable efforts to inform others (including people you name) of the amendment and to include the changes in any future disclosures of that information.

Electronic Notice: If you view this Notice on our website or by electronic mail (e-mail), you are entitled to receive a copy of this Notice in written form. Please contact us as directed below to obtain this Notice in written form.

Security of Your Information

Houston Honorary Hospital safeguards customer information using various tools such as firewalls, passwords, and data encryption. We continually strive to improve these tools to meet or exceed industry standards. We also limit access to your information to protect against its unauthorized use. The only **Houston Honorary Hospital** workforce members who have access to your information are those who need it as part of their job. These safeguards help us meet both federal and state requirements to protect your personal health information.

Questions or Concerns

If you would like more information about our privacy practices or have questions or concerns about this Notice, please contact the Privacy Office at the number listed below. If you believe your privacy rights have been violated, you may file a complaint, in writing, to the Houston Honorary Hospital Privacy Office located at

99999 Freeway, Suite 999
Houston, Texas 99999
or by calling 1-999-999-9999.

Or you may contact the U.S. Department of Health and Human Services (DHHS)
00000 Young Street, Suite 00000
Houston, Texas 99999
Voice Phone 000-000-0000
FAX 000-000-0000
TDD 000-000-0000

To e-mail the DHHS Secretary or other Department Officials, send your message to hhs@mail@os.dhhs.gov.

Figure 3-6 Sample Notice of Privacy Practices (continued)

17. Right to Request a Restriction of Uses and Disclosures

- a.** HIPAA Omnibus Rule affirms an individual's right to restrict the disclosure of his or her information to a health plan where
 - i.** The disclosure is for healthcare operations or payment and disclosure is not otherwise required by law
 - ii.** The PHI relates solely to a product or service for which the individual or a third party paid in full, out of pocket
- b.** Upon such a request, covered entities must comply with such a restriction and must not disclose the restricted information to the individual's health plans.
- c.** Business associates of a health plan are equally prohibited from receiving the restricted PHI.
- d.** Omnibus Rule gives covered entities guidance on how to comply with this provision.
 - i.** Covered entities are not required to take the time to separate the restricted records, but DHHS does require them to flag or make notes to records to identify restricted PHI.
 - ii.** Covered entities should understand how this flag works within their own electronic health records.
 - iii.** Where covered entities cannot "unbundle" their services, they must explain this to the individual, and if there is no way to restrict the PHI for just one service or product, all services or products in the bundle must be restricted.
 - iv.** DHHS emphasizes that it is the mandatory duty of covered entities to unbundle and restrict the PHI where they can.
 - v.** As a protection for the covered entity, where a payment to the covered entity fails (e.g., bounced check), the covered entity can contact and disclose all relevant information to the health plan to secure payment, but only after it tries to remedy the situation with the individual, such as by a phone call seeking an alternative form of payment.
 - vi.** Covered entities are allowed to disregard the restriction where the provider needs to justify follow-up care that was not paid out of pocket.

18. Individuals' Right of Access to PHI

- a.** Privacy Rule has always emphasized the importance of allowing individuals to have access to their own PHI.
- b.** HIPAA Omnibus Rule requires that covered entities provide individuals with a copy of the PHI that is maintained in a designated record set in the form and format requested by the individual; if that is not possible, it must reach an agreement with the individual for the provision of that information electronically.
- c.** The requested information must be provided within 30 days.
- d.** Covered entities are allowed one 30-day extension if circumstances warrant a delay.
- e.** Individuals may designate third parties to receive their information, and the covered entity is required by the HIPAA Omnibus Rule to send the information to that person upon a signed written request.
- f.** Covered entities are not required to investigate each request to ensure the third party seeking the records is doing so honestly.
- g.** Covered entities must have policies and procedures in place to verify the third party's identity when they request access to the PHI, as well as to protect the PHI as it is shared.

- h.** Covered entities may charge fees for their efforts in response to a request for information, but the fee must be based on the actual costs incurred to provide the information.
- i.** For paper records, the fee can include only the costs of supplies and labor, postage, and preparation of a summary of the contents.
- j.** For electronic records, the fee can include labor costs, and, where requested by the individual, the costs for the electronic media on which the records are transferred (such as a CD or a USB drive), postage (where the electronic media is mailed), and a summary of the contents.
- k.** The covered entity cannot allocate computer costs or data storage costs to the fee.

19. Fundraising

- a.** These changes are both more permissive and more restrictive than the previous standards.
- b.** Rule is more permissive: covered entities have significant flexibility in how they fundraise and how they offer individuals the opportunity to opt out.
- c.** Rule is more restrictive: it prohibits a covered entity from sending fundraising communications once the individual has opted out of receiving such communications.

20. Marketing

- a.** If the covered entity is receiving payment from a third party for making a “subsidized communication,” then the covered entity must obtain authorizations; there are no longer any exceptions in this case.
- b.** Because an authorization for each “subsidized communication” is now required, covered entities do not have to include information about these communications in their notices of privacy practices (NPPs).
- c.** Covered entities do not have to include information in their NPPs about appointment reminders, treatment alternatives, and other services, which are for treatment and operations.
- d.** The authorization is valid where it meets the general requirements for all HIPAA authorizations and tells the individual he or she may revoke the permission at any time.
- e.** The authorization must notify the individual that a third party is paying the covered entity to make the communication. Such notice may be either general or situation- or product-specific, but must at least give the individual an idea of the intended purpose of the use or disclosure.
- f.** HIPAA Omnibus Rule: exception for refill reminders, adherence reminders, and delivery system instructions. As long as the remuneration received by the covered entity is reasonably related to the cost of making the communication, and the covered entity does not make a profit, such reminders are not considered marketing communications.

21. Sale of PHI

- a.** Pursuant to HITECH Act, a covered entity cannot “sell” an individual’s PHI without the individual’s authorization.
- b.** HIPAA Omnibus Rule clarifies that “sale of PHI” includes a covered entity or business associate receiving, directly or indirectly, financial or nonfinancial remuneration in exchange for PHI.
- c.** A change in ownership of the PHI is not required, and a lease, license, or even access might trigger the protections in this provision.
- d.** Several exceptions protect many legitimate arrangements.
 - i.** For instance, the “sale of PHI” does not include disclosures for public health purposes, treatment, or operations.

- ii. Perhaps the largest exception is for disclosures by a covered entity or a business associate, in accordance with the Privacy Rule, for a reasonable, cost-based fee.
 - e. If a covered entity or business associate will be receiving remuneration in exchange for PHI, it should evaluate the arrangement to ensure it meets an exception.
 - f. If it does not, then the covered entity will have to secure the individual's authorization before proceeding.
- 22. Decedents, 50-Year Release**
- a. The current HIPAA Privacy Rule requires covered entities to continue protecting the privacy of PHI indefinitely after an individual's death.
 - b. This causes hardship for historians and other researchers who cannot access records due to HIPAA protections.
 - c. HIPAA Omnibus Rule modifies the requirement so that the privacy protections apply for only 50 years after the date of death.
 - d. DHHS emphasizes that this change does not displace stricter state or other laws, or the professional responsibility of medical providers.
 - e. The change is not a mandate that entities keep their records for that long; HIPAA does not have record retention requirements.
- 23. Decedents, Disclosures to a Family Member/Others Involved in Care**
- a. Changes to this section of the Privacy Rule arose from frustrations of family members of decedents who were unable to access information related to the death of their loved one.
 - b. HIPAA Omnibus Rule allows covered entities to disclose the decedent's PHI to a family member or other person involved in the decedent's care or treatment, but only to the extent the PHI is relevant to the role the family member or other person played in the decedent's treatment.
 - c. No release is permissible where the individual expressly stated before death that he or she preferred the PHI not be released.
 - d. This is not a requirement, but rather a permission; if the covered entity doubts the identity or explanation of the person seeking the information, it may deny the request.
- 24. Student Immunization in Schools**
- a. HIPAA Omnibus Rule allows covered entities in states that have compulsory vaccination laws to disclose immunization records to schools without obtaining formal parental authorization.
 - b. A covered entity must simply obtain permission, which can be oral or written, and such permission documented in the covered entity's records.
 - c. Does not change the fact that disclosures to immunization databases are considered public health disclosures, so no authorization is required.
 - d. This part of the Omnibus Rule does not affect any state laws. If state law requires authorization for this type of disclosure, HIPAA does not preempt that state law.
- 25. Expansion of Rule's Application: Definition of Business Associate**
- a. Inclusion of Subcontractors
 - i. 2013 Amendments significantly expand the definition of a business associate to include subcontractors of business associates (and their subcontractors) that create, receive, maintain, or transmit PHI in performing a function, activity, or service delegated by the business associate to a subcontractor.
 - ii. A covered entity must obtain satisfactory assurances in the form of a written contract or other arrangement from each business associate, and each business associate must do the same with

regard to each subcontractor that handles PHI on its behalf, and so on—no matter how far “down the chain” the PHI flows.

- b. Inclusion of Health Information Organizations, Vendors of Personal Health Records, and Others That Facilitate Data Transmission**
 - i.** Included in the definition of a business associate are entities that create, receive, maintain, or transmit PHI through electronic means, such as health information organizations (HIOs); vendors of personal health records; and others that facilitate data transmission.
- c. Compliance Deadlines for Business Associate Compliance**
 - i.** Modified Breach Standard and Notification Rule
 - ii.** Breach: under current interim rule, defined as an inappropriate use or disclosure of PHI involving a significant risk of financial, reputational or other harm.
 - iii.** 2013 Amendments modify this definition by providing that an impermissible use or disclosure of PHI is presumed to be a breach, unless it can be demonstrated that there is a low probability that PHI has been compromised based upon a four-part risk assessment that considers:
 - 1.** The nature and extent of the PHI involved in the breach
 - 2.** The unauthorized person who used the PHI or to whom the disclosure was made
 - 3.** Whether the PHI was actually acquired or viewed
 - 4.** The extent to which the risk to PHI has been mitigated
 - iv.** If the risk assessment evaluation fails to demonstrate there is a low probability that any PHI has been compromised, breach notification is required.
 - v.** Certain exceptions to the definition of a breach continue to apply.
- d. Notification**
 - i.** 2013 Amendments require covered entities to notify each affected individual whose unsecured PHI has been compromised.
 - ii.** Even if such breach is caused by a business associate, the covered entity is ultimately responsible for providing the notification (although the covered entity is free to delegate the breach response function to the business associate).
 - iii.** A business associate’s, and the workforce member’s, knowledge of a breach will be imputed onto a covered entity.
 - iv.** If the breach involves more than 500 persons, OCR must be notified in accordance with instructions posted on its website.
 - v.** The HIPAA-covered entity bears the ultimate burden of proof to demonstrate that all notifications were given or that the impermissible use or disclosure of PHI did not constitute a breach.
 - vi.** The covered entity must maintain supporting documentation, including documentation pertaining to the risk assessment.

26. Security Rule

- a.** HIPAA Security Rule applies to electronic PHI (e-PHI) that is created, received, maintained, or transmitted by a covered entity.
- b.** 2013 Amendments expand the application of the Security Rule to business associates (now defined to include subcontractors of business associates that handle PHI for or on behalf of business associates).
- c.** Business associates must comply with all of the Security Rule’s applicable administrative safeguards (e.g., security management procedures, training), physical safeguards (e.g., workstation security, device

and media controls), and technical safeguards (e.g., audit controls, transmission security).

- d. Business associates, including their subcontractors that handle PHI, must enter into agreements that require the business associates to comply with the Security Rule.
- e. A downstream business associate (or a business associate subcontractor) must notify the upstream entity of any security incident or breach under the breach notification rules.

27. Notice of Privacy Practices

- a. 2013 Amendments reflect modifications from the interim final rule that provide significant changes to covered entities' NPP regarding uses and disclosures that require authorization.
- b. While 2013 Amendments do not require the NPP to include all situations requiring authorization, the NPP must contain a statement indicating that most uses and disclosures of psychotherapy notes, marketing disclosures, and sale of PHI do require prior authorization, as well as the right of the individual to be notified in case of a breach of unsecured PHI.

28. Modifications to the HIPAA Privacy Rule Under GINA

- a. Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits discrimination based on an individual's genetic information.

29. Legislation/Regulation Trends Impacting HIM

- a. Accountable care organization (ACO) changes:
 - i. Requires new method for information exchange and need for quality data to ensure effective and coordinated patient care
 - ii. Describes how data will be managed, shared, and protected
- b. Big Data: managing upcoming torrent of data from hospitals and other care settings; HIM professional plays a major role in evaluating and determining use
- c. Health information exchange (HIE): effective sharing of information across the continuum of care
- d. Longitudinal coordination of care: focus placed on long-term and post-acute-care settings to improve outcomes while decreasing hospital readmissions
- e. E-discovery: advanced technology and new regulations (such as HITECH Act) describe the process by which each party in a lawsuit will obtain and view electronically stored information
- f. Healthcare reform: ties reimbursement to quality of care
 - i. Readmission rates, patient satisfaction scores, and other data-driven outcomes measures will play a major role in reimbursement
 - ii. Increased quality monitoring and reporting
 - iii. Expected to boost the need for highly trained HIM professionals
 - iv. HIM professionals required to implement HIM-related policies mandated by the federal government

Table 3-7
Stage 1 versus Stage 2
Comparison Table for Eligible Hospitals and CAHs

Last Updated: August 2012

Core Objectives (16 total)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Use CPOE for medication orders directly entered by any licensed healthcare professional who can enter orders into the medical record per state, local, and professional guidelines	More than 30% of unique patients with at least one medication in their medication list admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one medication order entered using CPOE	Use computerized provider order entry (CPOE) for medication, laboratory, and radiology orders directly entered by any licensed healthcare professional who can enter orders into the medical record per state, local, and professional guidelines	More than 60% of medication, 30% of laboratory, and 30% of radiology orders created by authorized providers of the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) during the EHR reporting period are recorded using CPOE
Implement drug–drug and drug–allergy interaction checks	The eligible hospital/CAH has enabled this functionality for the entire EHR reporting period	<i>No longer a separate objective for Stage 2</i>	<i>This measure is incorporated into the Stage 2 Clinical Decision Support measure</i>
Record demographics <ul style="list-style-type: none"> • Preferred language • Gender • Race • Ethnicity • Date of birth • Date and preliminary cause of death in the event of mortality in the eligible hospital or CAH 	More than 50% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have demographics recorded as structured data	Record the following demographics <ul style="list-style-type: none"> • Preferred language • Gender • Race • Ethnicity • Date of birth • Date and preliminary cause of death in the event of mortality in the eligible hospital or CAH 	More than 80% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have demographics recorded as structured data

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Maintain an up-to-date problem list of current and active diagnoses	More than 80% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one entry or an indication that no problems are known for the patient recorded as structured data	<i>No longer a separate objective for Stage 2</i>	<i>This measure is incorporated into the Stage 2 measure of Summary of Care Document at Transitions of Care and Referrals</i>
Maintain active medication list	More than 80% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one entry (or an indication that the patient is not currently prescribed any medication) recorded as structured data	<i>No longer a separate objective for Stage 2</i>	<i>This measure is incorporated into the Stage 2 measure of Summary of Care Document at Transitions of Care and Referrals</i>
Maintain active medication allergy list	More than 80% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one entry (or an indication that the patient has no known medication allergies) recorded as structured data	<i>No longer a separate objective for Stage 2</i>	<i>This measure is incorporated into the Stage 2 measure of Summary of Care Document at Transitions of Care and Referrals</i>

(continues)

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Record and chart changes in vital signs: <ul style="list-style-type: none"> • Height • Weight • Blood pressure • Calculate and display BMI • Plot and display growth charts for children 2–20 years, including BMI 	More than 50% of all unique patients age 2 and over admitted to eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23), blood pressure, height, and weight are recorded as structured data	Record and chart changes in vital signs: <ul style="list-style-type: none"> • Height • Weight • Blood pressure (age 3 and over) • Calculate and display BMI • Plot and display growth charts for patients 0–20 years, including BMI 	More than 80% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have blood pressure (for patients age 3 and over only) and height and weight (for all ages) recorded as structured data
Record smoking status for patients 13 years old or older	More than 50% of all unique patients 13 years old or older admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have smoking status recorded as structured data	Record smoking status for patients 13 years old or older	More than 80% of all unique patients 13 years old or older admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have smoking status recorded as structured data
Implement one clinical decision support rule relevant to specialty or high clinical priority along with the ability to track compliance that rule	Implement one clinical decision support rule	Use clinical decision support to improve performance on high-priority health conditions	1. Implement five clinical decision support interventions related to four or more clinical quality measures, if applicable, at a relevant point in patient care for the entire EHR reporting period. 2. The eligible hospital or CAH has enabled the functionality for drug–drug and drug–allergy interaction checks for the entire EHR reporting period

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Report clinical quality measures (CQMs) to CMS or the States	For 2011, provide aggregate numerator, denominator, and exclusions through attestation or electronically through the Hospital Reporting Pilot	<i>No longer a separate objective for Stage 2, but providers must still submit CQMs to CMS or the States to achieve meaningful use</i>	<i>Starting in 2014, all CQMs will be submitted electronically to CMS.</i>
Provide patients with an electronic copy of their health information (including diagnostic test results, problem list, medication lists, medication allergies), upon request	More than 50% of all patients of the inpatient or emergency departments of the eligible hospital or CAH (POS 21 or 23) who request an electronic copy of their health information are provided it within 3 business days	Provide patients the ability to view online, download, and transmit their health information within 36 hours after discharge from the hospital	<ol style="list-style-type: none"> 1. More than 50% of all unique patients discharged from the inpatient or emergency departments of the eligible hospital or CAH (POS 21 or 23) during the EHR reporting period are provided timely (available to the patient within 36 hours after discharge from the hospital) online access to their health information 2. More than 5% of all unique patients discharged from the inpatient or emergency departments of the eligible hospital or CAH (POS 21 or 23) during the EHR reporting period (or their authorized representatives) view, download, or transmit to a third party their health information

(continues)

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request	More than 50% of all patients who are discharged from an eligible hospital or CAH's inpatient department or emergency department (POS 21 or 23) and who request an electronic copy of their discharge instructions are provided it	<i>This objective is eliminated from Stage 1 in 2014 and is no longer a separate objective for Stage 2</i>	<i>This measure has been incorporated into the View, Download, and Transmit objective for Stage 2</i>
Capability to exchange key clinical information (for example, problem list, medication list, medication allergies, diagnostic test results), among providers of care and patient authorized entities electronically	Performed at least one test of Certified EHR Technology's capacity to electronically exchange key clinical information	<i>This objective is eliminated from Stage 1 in 2013 and is no longer an objective for Stage 2</i>	<i>This measure is eliminated from Stage 1 in 2013 and is no longer a measure for Stage 2</i>
Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities	Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/ security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Implement drug-formulary checks	The eligible hospital/CAH has enabled this functionality and has access to at least one internal or external drug formulary for the entire EHR reporting period	<i>No longer a separate objective for Stage 2</i>	<i>This measure is incorporated into the e-Prescribing measure for Stage 2</i>
Incorporate clinical lab test results into Certified EHR Technology as structured data	More than 40% of all clinical lab tests results ordered by an authorized provider of the eligible hospital or CAH for patients admitted to its inpatient or emergency department (POS 21 or 23) during the EHR reporting period whose results are either in a positive/negative or numerical format are incorporated in certified EHR technology as structured data	Incorporate clinical lab test results into Certified EHR Technology as structured data	More than 55% of all clinical lab tests results ordered by authorized providers of the eligible hospital or CAH for patients admitted to its inpatient or emergency department (POS 21 or 23) during the EHR reporting period whose results are either in a positive/negative or numerical format are incorporated in Certified EHR Technology as structured data
Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research or outreach	Generate at least one report listing patients of the eligible hospital or CAH with a specific condition	Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach	Generate at least one report listing patients of the eligible hospital or CAH with a specific condition

(continues)

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Use Certified EHR Technology to identify patient-specific education resources and provide those resources to the patient if appropriate	More than 10% of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) are provided patient-specific education resources	Use Certified EHR Technology to identify patient-specific education resources and provide those resources to the patient if appropriate	More than 10% of all unique patients admitted to the eligible hospital's or CAH's inpatient and emergency departments (POS 21 and 23) are provided patient-specific education resources identified by Certified EHR Technology
The eligible hospital or CAH that receives a patient from another setting of care or provider of care or believes an encounter is relevant should perform medication reconciliation	The eligible hospital or CAH performs medication reconciliation for more than 50% of transitions of care in which the patient is admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23)	The eligible hospital or CAH that receives a patient from another setting of care or provider of care or believes an encounter is relevant should perform medication reconciliation	The eligible hospital or CAH performs medication reconciliation for more than 50% of transitions of care in which the patient is admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23)
The eligible hospital or CAH that transitions its patient to another setting of care or provider of care or refers their patient to another provider of care should provide summary of care record for each transition of care or referral	The eligible hospital or CAH that transitions or refers its patient to another setting of care or provider of care provides a summary of care record for more than 50% of transitions of care and referrals	The eligible hospital or CAH that transitions its patient to another setting of care or provider of care or refers their patient to another provider of care should provide summary of care record for each transition of care or referral	<ol style="list-style-type: none"> 1. The eligible hospital, or CAH that transitions or refers its patient to another setting of care or provider of care provides a summary of care record for more than 50% of transitions of care and referrals 2. The eligible hospital or CAH that transitions or refers its patient to another setting of care or provider of care provides a summary of care record either (a) electronically transmitted to a recipient using

Table 3-7 Core Objectives (16 total) (continued)			
Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
			CEHRT or (b) where the recipient receives the summary of care record via exchange facilitated by an organization that is a NHIN Exchange participant or is validated through an ONC-established governance mechanism to facilitate exchange for 10% of transitions and referrals
		3. The eligible hospital or CAH that transitions or refers its patient to another setting of care or provider of care must either (a) conduct one or more successful electronic exchanges of a summary of care record with a recipient using technology that was designed by a different EHR developer than the sender's, or (b) conduct one or more successful tests with the CMS-designed test EHR during the EHR reporting period	

(continues)

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Capability to submit electronic data to immunization registries or immunization information systems, and actual submission except where prohibited and in accordance with applicable law and practice	Performed at least one test of Certified EHR Technology's capacity to submit electronic data to immunization registries and follow-up submission if the test is successful (unless none of the immunization registries to which the eligible hospital or CAH submits such information has the capacity to receive the information electronically)	Capability to submit electronic data to immunization registries or immunization information systems, and actual submission except where prohibited and in accordance with applicable law and practice	Successful ongoing submission of electronic immunization data from Certified EHR Technology to an immunization registry or immunization information system for the entire EHR reporting period
Capability to submit electronic data on reportable (as required by state or local law) lab results to public health agencies, and actual submission except where prohibited and in accordance with applicable law and practice	Performed at least one test of Certified EHR Technology's capacity to provide electronic submission of reportable lab results to public health agencies and follow-up submission if the test is successful (unless none of the public health agencies to which eligible hospital or CAH submits such information has the capacity to receive the information electronically)	Capability to submit electronic data on reportable (as required by state or local law) lab results to public health agencies, and actual submission except where prohibited and in accordance with applicable law and practice	Successful ongoing submission of electronic reportable laboratory results from Certified EHR Technology to public health agencies for the entire EHR reporting period as authorized, and in accordance with applicable state law and practice

Table 3-7 Core Objectives (16 total) (continued)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Capability to submit electronic syndromic surveillance data to public health agencies, and actual submission except where prohibited and in accordance with applicable law and practice	Performed at least one test of Certified EHR Technology's capacity to provide electronic syndromic surveillance data to public health agencies and follow-up submission if the test is successful (unless none of the public health agencies to which an eligible hospital or CAH submits such information has the capacity to receive the information electronically)	Capability to submit electronic syndromic surveillance data to public health agencies, and actual submission except where prohibited and in accordance with applicable law and practice	Successful ongoing submission of electronic syndromic surveillance data from Certified EHR Technology to a public health agency for the entire EHR reporting period
NEW	NEW	Automatically track medications from order to administration using assistive technologies in conjunction with an electronic medication administration record (eMAR)	More than 10% of medication orders created by authorized providers of the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) during the EHR reporting period for which all doses are tracked are tracked using eMAR

(continues)

Table 3-7 Menu Objectives (Eligible hospitals and CAHs must report on 3 of 6 menu objectives)

Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
Record advance directives for patients 65 years old or older	More than 50% of all unique patients 65 years old or older admitted to the eligible hospital's or CAH's inpatient department (POS 21) have an indication of an advance directive status recorded	Record whether a patient 65 years old or older has an advance directive	More than 50% of all unique patients 65 years old or older admitted to the eligible hospital's or CAH's inpatient department (POS 21) during the EHR reporting period have an indication of an advance directive status recorded as structured data
NEW	NEW	Record electronic notes in patient records	Enter at least one electronic progress note created, edited, and signed by an eligible provider for more than 30% of unique patients admitted to the eligible hospital or CAH's inpatient or emergency department during the EHR reporting period
NEW	NEW	Imaging results consisting of the image itself and any explanation or other accompanying information are accessible through CEHRT	More than 10% of all scans and tests whose result is an image ordered by an authorized provider of the eligible hospital or CAH for patients admitted to its inpatient or emergency department (POS 21 and 23) during the EHR reporting period are incorporated into or accessible through Certified EHR Technology

Table 3-7 Menu Objectives (continued)			
Stage 1 Objective	Stage 1 Measure	Stage 2 Objective	Stage 2 Measure
NEW	NEW	Record patient family health history as structured data	More than 20% of all unique patients admitted to the eligible hospital or CAH's inpatient or emergency department (POS 21 or 23) during the EHR reporting period have a structured data entry for one or more first-degree relatives or an indication that family health history has been reviewed
NEW	NEW	Generate and transmit permissible discharge prescriptions electronically (eRx)	More than 10% of hospital discharge medication orders for permissible prescriptions (for new or changed prescriptions) are compared to at least one drug formulary and transmitted electronically using Certified EHR Technology
NEW	NEW	Provide structured electronic lab results to ambulatory providers	Hospital labs send structured electronic clinical lab results to the ordering provider for more than 20% of electronic lab orders received

Reproduced from the Centers for Medicaid and Medicare Services (2012). Stage 1 vs. Stage 2 Comparison Table for Eligible Hospitals and CAHs. <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/stage1vsStage2CompTablesforHospitals.pdf>. Last Updated: August 2012. Accessed March 4, 2014.

PRACTICAL APPLICATION OF YOUR KNOWLEDGE

1. Answer the following questions on the organization of the legal system:

a. What are the three levels of the government and the sources or documents that outline their power?

1.

2.

3.

b. What are the three branches of federal and state government and their duties?

1.

2.

3.

c. Distinguish between public and private law. Which usually deals with disputes between patients and healthcare providers?

d. Discuss the rules of administrative agencies and give an example of an administrative agency that affects healthcare legislation.

2. Health Record Requirements and Retention Guidelines

- a. List the contents that should be included in an inpatient health record according to TJC.
- b. As manager of the health information department, you are constructing a retention schedule. Using AHIMA guidelines, state the length of time the following documents should be maintained:

Document	Retention Guideline
Adult patient health record	
Minor patient health record	
Diagnostic images (e.g., X-rays)	
Disease index	
Fetal heart monitor record	
Master patient index	
Operative index	
Physician index	
Register of births	
Register of deaths	
Register of surgical procedures	

3. Confidentiality, Consent, and Security of Health Records

- a. What is confidential information?
- b. Who is the owner of the health record?
- c. Who has the authority to release information from the health record?
- d. When is authorization not required to release PHI?
- e. What are the three elements of a privileged communication?
- f. State three types of consent.
- g. What is informed consent? What should be included in an informed consent?
- h. From what threats to the security of records must a health information practitioner protect those records?

4. Laws and Regulations Regarding Health Records

- a. Summarize the following federal legislation:

Legislation	Summary
Freedom of Information Act (1966)	
Drug Abuse and Treatment Act (1972)	
Privacy Act (1974)	
Natural Death Act (1989)	
Health Insurance Portability and Accountability Act (1996)	

5. Release of Information and Subpoenas

- a.** To meet HIPAA requirements, a Release of Information form must collect what information?

b. Subpoenas

- 1.** Match the term to its description or definition

- a.** Subpoena duces tecum
- b.** Subpoena ad testificandum
- c.** Contempt of court

- 1.** _____ Results when a person fails to obey a subpoena and is punishable by fine or imprisonment

- 2.** _____ Court order that commands a person to come to court and produce whatever documents are named in the order

- 3.** _____ Court order that requires a person to appear in court to testify

- c.** List eight common elements of a valid subpoena.

1.

2.

3.

4.

5.

6.

7.

8.

6. Health Insurance Portability and Accountability Act

- a.** Discuss the administration simplification provisions.

- b.** Discuss the Privacy Rule.

- c.** What is PHI?

- d.** Mark these statements concerning the HIPAA Privacy Rule as True or False.
 - 1.** _____ The HIPAA Privacy Rule protects a patient's fundamental right to privacy and confidentiality.
 - 2.** _____ A covered entity is a healthcare provider, health plan, or healthcare clearinghouse that transmits health information in electronic form.
 - 3.** _____ PHI is anything that connects a patient to his or her health information.
 - 4.** _____ After signing an authorization, the patient can decide to revoke it.
 - 5.** _____ An authorization must contain an expiration date.
 - 6.** _____ PHI includes all health information that is used or disclosed except PHI in oral form.
 - 7.** _____ The healthcare facility must obtain patient agreement to use or disclose PHI for public health activities related to disease prevention.
 - 8.** _____ In general, disclosure of PHI must be limited to the least amount needed to get the job done correctly.
 - 9.** _____ The Privacy Rule gives patients the right to take action if their privacy is violated.
 - 10.** _____ The Privacy Rule gives patients the right to request a history of routine disclosures.

7. Health Record Documentation

a. List 10 guidelines for documentation in the health record.

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

b. A physician charts the information of a patient in the wrong health record. Describe how the documentation can be corrected in each patient's record.

8. Health Records in Court

a. Describe the following steps:

Step	Description
Complaint	
Answers	
Motions	
Pretrial discovery	
Notice of trial	
Memorandum of law	

b. Describe the steps of the civil pretrial procedure.

c. A patient sues your facility for malpractice. Describe the steps in a legal proceeding by which this case may be decided from its beginning to its conclusion.

9. Malpractice and Negligence

- a.** Describe the four components that must be present for a plaintiff to recover damages caused by negligence.

1.

2.

3.

4.

10. Computer-Based Health Records

- a.** List five methods to secure computer-based health records from unauthorized access.

1.

2.

3.

4.

5.

11. Ethical Issues for Health Information Practitioners

a. List 10 ethical obligations of the health information practitioner.

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

12. Define the Following Terms:

- a.** Admissibility
- b.** Advance directive
- c.** Assault and battery
- d.** Business record rule
- e.** Evidence
- f.** Defamation
- g.** Defendant
- h.** Deposition
- i.** Hearsay
- j.** Interrogatory
- k.** Law
- l.** Libel

m. Malpractice

n. Negligence

o. Plaintiff

p. Res gestae

q. Res ipsa loquitur

r. Res judicata

s. Respondeat superior

t. Stare decisis

u. Statute of limitations

v. Tort

w. Venue

TEST YOUR KNOWLEDGE

Select the best answer for the questions or incomplete statements.

1. A nurse employed by your hospital gossiped about a discharged inpatient, which resulted in the patient's good reputation being questioned by his neighbor. This is known as what?
 - a. Libel
 - b. Slander
 - c. Perjury
 - d. Defamation
2. A third-party payer has requested copies of a patient's records. The patient has been diagnosed as having AIDS. The hospital's policy for release of information in this instance should ensure that the:
 - a. record is sent by overnight express.
 - b. physician gives consent for a copy of the record to be released.
 - c. a subpoena duces tecum is received from the third-party payer.
 - d. patient has signed a consent specifically authorizing release of this diagnosis.
3. A properly completed and signed authorization is required for release of all health information, except when a(n):
 - a. patient has died.
 - b. patient presents to the hospital with a highly contagious disease that must be reported to the state health department.
 - c. patient's spouse suspects the patient has AIDS and is afraid of contracting the disease.
 - d. insurance company request copies of the patient's previous hospitalization record.
4. Which of the following is an example of respondeat superior?
 - a. The hospital is held responsible for a pharmacist medication error.
 - b. A physician with honorary staff status is sued by a current inpatient for malpractice.
 - c. The director of nurses gives instructions to a staff nurse.
 - d. The attending physician testifies against the surgeon in a malpractice case.
5. You are the supervisor of release of information and have been subpoenaed to bring records to court. With what document may you have been served?
 - a. Subpoena duces tecum
 - b. Subpoena ad testificandum
 - c. Subpoena gestae
 - d. Subpoena respondeat
6. Refusing to honor a subpoena may result in:
 - a. the case being postponed.
 - b. arrest of the attending physician.
 - c. being held in contempt of court.
 - d. receiving a court order.
7. According to the American Health Information Management Association, the suggested retention schedule for the master patient index is how long?
 - a. 5 years
 - b. 10 years
 - c. 25 years
 - d. Permanently
8. The statute of limitation sets:
 - a. the maximum dollar amount that can be collected from a malpractice case.
 - b. standards for the maintenance of pharmaceuticals.
 - c. a minimum amount of time after an event occurs for a suit to be taken in court.
 - d. a time period for the completion of medical records.

9. As supervisor of release of information you have been subpoenaed to court. You are qualified to testify in response to a subpoena duces tecum as to:
 - a. the quality of care rendered by the medical staff to the patient.
 - b. how the health records are maintained in the facility's regular course of business.
 - c. the accuracy of a respiratory therapist's documentation.
 - d. whether the confidentiality of the health information has been violated.
10. In a nonemergent situation, protected health information may be released to another hospital with the:
 - a. written authorization of the patient.
 - b. permission of the attending physician.
 - c. death of the patient.
 - d. receipt of a phone call from the patient's spouse.
11. Which of the following demonstrates the doctrine of res ipsa loquitur?
 - a. A surgeon places a pacemaker in a patient.
 - b. A surgeon erroneously leaves an instrument in a patient.
 - c. A radiology technician takes an X-ray of the wrong leg of a patient.
 - d. A nurse neglects to give a patient her prescribed medication.
12. A patient has a primary diagnosis of alcohol abuse and dependence. What information may be released without express authorization of the patient?
 - a. Admission and discharge dates only
 - b. The patient's physical health status
 - c. The patient's attending physician's name
 - d. No information at all
13. TJC requests to view a patient's health record, which contains a diagnosis of AIDS. The director of health information should:
 - a. call the facility's attorney.
 - b. deny access to TJC.
 - c. obtain written authorization from the patient or legal representative.
 - d. allow access to the record upon request of TJC.
14. Which rule requires covered entities to assign a unique name and/or number for identifying and tracking user identity?
 - a. Privacy Rule
 - b. Security Rule
 - c. Administrative Rule
 - d. None of the above
15. Which of the following is required to be present in an informed consent?
 - a. Explanation of risks and benefits of treatment and or surgery
 - b. List of referral physicians to obtain another expert opinion
 - c. Alternative facilities that may treat the patient
 - d. Cost of treatment and surgery
16. A school representative brings a minor to the facility with a broken arm, which requires surgery. Who may consent to the treatment of the patient?
 - a. The school representative
 - b. The minor patient
 - c. The person with legal custody of the minor patient
 - d. No consent is necessary in the emergent situation.
17. In a physician-owned clinic, the health record is the property of the:
 - a. patient.
 - b. admitting physician.
 - c. physician-owned clinic.
 - d. hospital to which the physician has admitting privileges.

18. A hospital fails to obtain informed consent prior to surgery on a patient. Which of the following may the hospital have performed?
 - a. Slander and tort
 - b. Defamation and liability
 - c. Libel and tort
 - d. Assault and battery
19. Tort claims have to do with what?
 - a. Wrongful conduct that has caused harm in public law
 - b. Unauthorized treatment
 - c. Public and criminal wrongs
 - d. Breach of contract
20. Health records may be admitted into court as evidence due to the:
 - a. hearsay rule.
 - b. business records rule.
 - c. Privacy Act.
 - d. HIPAA.
21. The powers of the three branches of the federal government are documented in the:
 - a. United States Constitution.
 - b. Act of Congress.
 - c. administrative law.
 - d. Articles of the Republic.
22. Bob brings a lawsuit against Houston Hospital for damages done to his knee during surgery. What term best describes Bob?
 - a. Defendant
 - b. Bailiff
 - c. Plaintiff
 - d. Attorney
23. Susan brings a lawsuit against Houston Hospital for wrongfully damaging her knee during surgery. What is this wrongful act called?
 - a. Tort
 - b. Slander
 - c. Libel
 - d. Assault
24. Austin Hospital is closed and sold to Houston Hospital. Which of the following entities owns the physical hospital health record?
 - a. The patients
 - b. Houston Hospital
 - c. Austin Hospital
 - d. The physicians who treated the patients
25. HIPAA Privacy Rules:
 - a. take precedence over all other federal and state laws.
 - b. are not relevant to children's hospitals.
 - c. provide a federal foundation for privacy requirements of health information.
 - d. are not subject to state laws.
26. PHI refers to _____ health information.
 - a. private
 - b. protected
 - c. previous
 - d. preliminary
27. Authorizations are always required for the use or disclosure of psychotherapy notes except in which of the following situations:
 - a. health insurance carrier
 - b. carry out payment, treatment, and operations
 - c. employee- and employment-related activities
 - d. media-related activities
28. Steve has submitted a written authorization to request a copy of his medical chart. However, Steve's psychiatrist has determined that access to his PHI might endanger his life or safety. What should the covered entity do concerning the request?
 - a. Provide an appeals process to Steve for the denial
 - b. Confirm the psychiatrist decision and deny the request
 - c. Release requested information to Steve's legal guardian
 - d. Release requested information to Steve

- 29. In regard to a patient's request for his PHI, which of the following statements is true?**
- a. A cost-based fee may be charged to view the PHI.
 - b. No fee may be charged for PHI.
 - c. A cost-based fee may be charged for personnel expenses.
 - d. A cost-based fee may be charged for making a copy of the PHI.
- 30. Steve submits a written request to Houston Hospital for a copy of his PHI on August 19. By what date must the covered entity comply?**
- a. August 29
 - b. September 3
 - c. September 8
 - d. September 18
- 31. Nurse Cecile makes an error in a patient's medical chart. What should she do?**
- a. Remove the page with the error
 - b. Obliterate the error
 - c. Line through the error, then add her correction, stating "correction" or "error"
 - d. Remove the page with error and add page with correction
- 32. Jennifer submits a written request to Houston Hospital for a copy of her PHI on August 19. The information is stored offsite. By what date must the covered entity comply?**
- a. August 29
 - b. September 19
 - c. September 30
 - d. October 18
- 33. Where can patients find a complete description of how PHI is used in a healthcare facility?**
- a. Notice of privacy practice
 - b. Medical staff rules and regulations
 - c. Governing board bylaws
 - d. HIM policies and procedures
- 34. The notice of privacy practice:**
- a. provides patients with a fee scale of private rooms.
 - b. must be provided to every individual at the first time of contact or service with the covered entity.
 - c. gives the covered entity permission to release information to private insurance companies.
 - d. explains to patients that the facility is a private institution and provides services on a fee-for-service basis.
- 35. The directory of patients maintained by a covered entity:**
- a. requires patients to maintain their name and room number in the directory.
 - b. allows patients to restrict information maintained on them in the directory.
 - c. may not be released.
 - d. must be maintained for 5 years.
- 36. Sworn testimony usually collected before a trial is a(n):**
- a. subpoena.
 - b. tort.
 - c. deposition.
 - d. complaint.
- 37. Bob brings a lawsuit against Houston Hospital for damages done to his knee during surgery. What term best describes Houston Hospital?**
- a. Defendant
 - b. Bailiff
 - c. Plaintiff
 - d. Complaintee
- 38. The MPI (master patient index) serves which of the following purposes?**
- a. Links to the patient record and facilitates patient identification that is critical to the quality and safety of patient care
 - b. Influences retention of patient medical records
 - c. Means of identifying off-site storage and retrieval methods
 - d. Maintains a longitudinal patient record from birth to death

39. With proper written authorization from a patient, Houston Hospital obtains a copy of the patient's health record from Austin Hospital. Houston Hospital then releases the information from Austin Hospital to Dallas Hospital. What is this practice called?
 - a. Redisdisclosure
 - b. Release of information
 - c. Voir dire
 - d. Ad testificandum
40. With proper written authorization from a patient, Houston Hospital obtains a copy of the patient's health record from Austin Hospital. Houston Hospital then releases the information from Austin Hospital to Dallas Hospital. This practice is:
 - a. never appropriate, because medical information should not be redisclosed.
 - b. mandated by HIPAA to ensure continuity of patient care.
 - c. regularly practiced due to the threat of medical lawsuits.
 - d. noncompliant with HIPAA, but compliant with FIOA.
41. Which of the following subpoenas will require the director of medical records to personally appear in court and produce documents and other records?
 - a. Subpoena ad testificandum
 - b. Subpoena duces in tecum
 - c. Subpoena to quash
 - d. None of the above
42. As a witness for Houston Hospital, the health information manager should:
 - a. refuse to turn over copies of medical records to the court that demonstrate negligence on the part of the hospital.
 - b. never tell the court that medical records were not able to be retrieved or were lost.
 - c. give copies of medical records to constable upon request.
 - d. refuse to turn over copies of medical records to the court without a subpoena duces tecum or court order.
43. Public health laws mandate reporting of certain diseases, which do not require the patient's consent for release of this information. These include:
 - a. deaths and herpes.
 - b. births and viral meningitis.
 - c. births and cancer cases.
 - d. deaths and viral meningitis.
44. An incompetent adult is an individual who is no longer capable of controlling his or her action due to all EXCEPT which of the following?
 - a. Injury
 - b. Illness
 - c. Disability
 - d. All of the above
45. Manuel was in a severe car accident and unable to grant permission for treatment. Therefore, his wife:
 - a. must obtain legal guardianship to speak for patient.
 - b. has no right to consent to or deny treatment for Manuel.
 - c. must obtain legal counsel to represent Manuel.
 - d. may give consent for his treatment.
46. Nipa was admitted to a Houston Community Hospital for gallbladder removal. Which of the following information about her is considered confidential?
 - a. Previous history and treatment of a concussion
 - b. Date of birth
 - c. Address upon admission
 - d. All information is considered confidential
47. Jim is 15 years old when treated for appendicitis with subsequent appendectomy. At what age will Jim be when his records may be destroyed, if the state's age of majority is 18 years of age?
 - a. 18
 - b. 25
 - c. 28
 - d. 30

- 48.** LaToya, a 16-year-old student, is hospitalized for pneumonia. She was ambulatory and mentally competent upon admission. LaToya is a married mother of two. Her mother is contacted to be informed of her daughter's status. Who may authorize treatment for LaToya?
- a.** LaToya
 - b.** LaToya's mom
 - c.** LaToya's husband
 - d.** No consent is required in an emergent situation.
- 49.** Bob, a 93-year-old male, was admitted and treated for a myocardial infarction. Due to his history of Alzheimer's disease, his daughter is his legal guardian. Bob lives with his son. Upon discharge from the hospital, his primary physician requests copies of his medical record. Who is required to sign an authorization for release of the medical record information to the physician?
- a.** Bob
 - b.** Bob's daughter
 - c.** Bob's son
 - d.** Due to continuity of care, an authorization is not mandatory.
- 50.** Of the following, which requestor is NOT required to submit the patient's written authorization to obtain copies of the patient's medical record from the hospital?
- a.** The patient
 - b.** The patient's attorney
 - c.** The patient's physician
 - d.** The hospital's attorney