

# Legal and Regulatory Issues

Prepared by Dr. Hayat Farag

MHA631  
Health Insurance

## Lecture 4



# Objectives

- Understand Legal and Regulatory Considerations.
- Explore Retention of Records.
- Discuss the Provisions of Health Insurance Portability and Accountability Act (HIPAA), such as fraud and abuse guidelines, electronic health information transaction standards, and privacy and security standards for health information.

## Introduction to Legal and Regulatory Considerations

- The health insurance specialist must be knowledgeable about laws and regulations for maintaining patient records and processing health insurance claims.
- **Federal and state statutes (or statutory law)** are laws passed by legislative bodies (e.g., federal Congress and state legislatures).
- These laws are then implemented as regulations, which are guidelines written by administrative agencies (e.g., CMS).

## Introduction to Legal and Regulatory Considerations

- Federal laws and regulations affect health care in that they govern programs such as Medicare, Medicaid, TRICARE, and the Federal Employees Health Benefit Plans (FEHBP).
- State laws regulate insurance companies, recordkeeping practices, and provider licensing.
- State insurance departments determine coverage issues for insurance policies (contracts) and state workers' compensation plans.

## Introduction to Legal and Regulatory Considerations

- **Civil law** deals with all areas of the law that are not classified as criminal.
- **Criminal law** is public law (statute or ordinance) that defines crimes and their prosecution.
- A **subpoena** is an order of the court that requires a witness to appear at a particular time and place to testify. A **subpoena duces tecum** requires documents (e.g., patient record) to be produced. A subpoena is used to obtain witness testimony at trial and at **deposition**, which is testimony under oath taken outside of court (e.g., at the provider's office).

## Introduction to Legal and Regulatory Considerations

- In civil cases (e.g., malpractice), the provider might be required to complete an **interrogatory**, which is a document containing a list of questions that must be answered in writing.
- The Federal Register is a legal newspaper published every business day by the National Archives and Records Administration (NARA). It is available in paper form, on microfiche, and online.

# Retention of Records



# Retention of Records

- **Record retention** is the storage of documentation for an established period of time, usually mandated by federal and/or state law.
- Its purpose is to ensure the availability of records for use by government agencies and other third parties (e.g., insurance audit, quality of care review).
- It is acceptable to store medical records and insurance claims (including attachments submitted to third-party payers) in a format other than original hard copy if the storage medium (e.g., microfilm, scanned images) accurately reproduces all original documents.

# Retention of Records

- The Health Insurance Portability and Accountability Act (HIPAA) mandates the retention of health insurance claims and accounting records for a minimum of 6 years, unless state law specifies a longer period.
- HIPAA also mandates that health insurance claims be retained for a minimum of 2 years after a patient's death.

# Retention of Records

**EXAMPLE 1:** Community Hospital is located in North Carolina (NC), which mandates that hospital medical records be retained for a minimum of 11 years following the discharge of an adult, and for a minor the record must be retained until the patient's 30th birthday. Because NC law is stricter than the HIPAA mandate regarding retention of records, Community Hospital must retain adult patient records for a period of 11 years and minor patient records until the patient's 30th birthday.

# Retention of Records

**EXAMPLE 2:** Dr. Smith practices in Delaware (DE), which mandates that medical records be retained for 5 years. Because the HIPAA mandate is stricter than DE state law, Dr. Smith must retain patient records for a period of 7 years. For any patient who has died, Dr. Smith must retain the record for a period of 2 years after the date of death.

# **Health Insurance Portability and Accountability Act (HIPAA)**

## Health Insurance Portability and Accountability Act (HIPAA)

- In 1996 Congress passed the Health Insurance Portability and Accountability Act (HIPAA) because of concerns about fraud, such as:
  - coding irregularities,
  - medical necessity issues, and
  - waiving of copays and deductibles.

## Preventing Healthcare Fraud and Abuse

- HIPAA defines **fraud** as “an intentional deception or misrepresentation that someone makes, knowing it is false, that could result in an unauthorized payment.”
- **Abuse** “involves actions that are inconsistent with accepted, sound medical, business, or fiscal practices. Abuse directly or indirectly results in unnecessary costs to the program through improper payments.”
- The difference between fraud and abuse is the individual’s intent; however, both have the same impact in that they steal valuable resources from the healthcare industry.

## Preventing Healthcare Fraud and Abuse

- The most common forms of Medicare **fraud** include
  - Billing for services not furnished.
  - Misrepresenting the diagnosis to justify payment.
  - Soliciting, offering, or receiving a kickback.
  - Unbundling codes (reporting multiple CPT codes to increase reimbursement, when a single combination code should be reported).
  - Falsifying certificates of medical necessity, plans of treatment, and medical records to justify payment.

## Preventing Healthcare Fraud and Abuse

- Examples of **abuse** include:
- Excessive charges for services, equipment, or supplies.
- Submitting claims for items or services that are not medically necessary to treat the patient's stated condition.
- Improper billing practices that result in a payment by a government program when the claim is the legal responsibility of another third-party payer.
- Violations of participating provider agreements with insurance companies.

## Preventing Healthcare Fraud and Abuse

- When a Medicare provider commits fraud, an investigation is conducted by the Department of Health and Human Services (DHHS) Office of the Inspector General (OIG).
- The OIG Office of Investigations prepares the case for referral to the Department of Justice for criminal and/or civil prosecution.

## Preventing Healthcare Fraud and Abuse

- A person found guilty of Medicare fraud faces criminal, civil, and/or administrative sanction penalties, including:
  - Civil penalties of \$5,000 to \$10,000 per false claim plus triple damages under the False Claims Act. (The provider pays an amount equal to three times the claim submitted, in addition to the civil penalties fine.)
  - Criminal fines and/or imprisonment of up to 10 years if convicted of the crime of healthcare fraud as outlined in HIPAA.

## Preventing Healthcare Fraud and Abuse

- Administrative sanctions, including up to a \$10,000 civil monetary penalty per line item on a false claim, assessments of up to triple the amount falsely claimed, and/or exclusion from participation in Medicare and state healthcare programs.

## Preventing Healthcare Fraud and Abuse

**EXAMPLE:** Medical review of claims submitted to Medicare by a physician group practice that contains mental health providers identified a pattern of psychiatric services billed on behalf of nursing facility patients with a medical history of dementia. Review of patient records revealed no mental healthcare physician orders or plans of treatment. This is an example of billing for services not furnished.

## Preventing Healthcare Fraud and Abuse

- By law, physicians are not subject to civil, administrative, or criminal penalties for innocent errors, or even negligence. The civil False Claims Act covers only offenses that are committed with actual knowledge of the falsity of the claim, or reckless disregard or deliberate ignorance of the truth or falsity of a claim. (The False Claims Act does not cover mistakes, errors, or negligence.)

## Preventing Healthcare Fraud and Abuse

- The OIG has stated that it is mindful of the difference between innocent errors (e.g., erroneous claims) and reckless or intentional conduct (e.g., fraudulent claims).
- A **voluntary compliance program** can help physicians avoid generating erroneous and fraudulent claims by ensuring that submitted claims are true and accurate, expediting and optimizing proper payment of claims, minimizing billing mistakes, and avoiding conflicts with self-referral and antikickback statutes.

## Preventing Healthcare Fraud and Abuse

- The final physician guidance by OIG identifies **four specific compliance risk areas** for physicians:
  - (1) proper coding and billing;
  - (2) ensuring that services are reasonable and necessary;
  - (3) proper documentation; and
  - (4) avoiding improper inducements, kickbacks, and self-referrals.
- These risk areas reflect areas in which the OIG has focused its investigations and audits related to physician practices.

# Overpayments



# Overpayments

- **Overpayments** are funds a provider or beneficiary receives in excess of amounts due and payable under Medicare and Medicaid statutes and regulations.
- Once a determination of overpayment has been made, the amount so determined is a debt owed to the United States government.

# Overpayments

- Examples of overpayments include:
  - Payment based on a charge that exceeds the reasonable charge.
  - Duplicate processing of charges/claims.
  - Payment to a physician on a non-assigned claim or to a beneficiary on an assigned claim (payment made to wrong payee).
  - Payment for non-covered items and services, including medically unnecessary services.
  - Incorrect application of the deductible or coinsurance.

# Overpayments

- Examples of overpayments include:
  - Primary payment for items or services for which another entity is the primary payer.
  - Payment for items or services rendered after the beneficiary's date of death (post-payment reviews are conducted to identify and recover payments with a billed date of service that is after the beneficiary's date of death).

# Overpayments

- When a Medicare administrative contractor determines that an overpayment was made, it proceeds with recovery by issuing an overpayment demand letter to the provider.
- The letter contains information about the review and statistical sampling methodology used as well as corrective actions to be taken.
- Corrective actions include payment suspension, imposition of civil money penalties, institution of pre- or post-payment review, additional edits, and so on.

# Overpayments

- Medicare administrative contractors are prohibited from seeking overpayment recovery when the following two time limitations apply:
- Overpayment is not reopened within 4 years (48 months) after the date of payment, unless the case involves fraud or similar fault.
- Overpayment is discovered later than three full calendar years after the year of payment, unless there is evidence that the provider or beneficiary was at fault with respect to the overpayment.

# Electronic Healthcare Transactions



# Electronic Healthcare Transactions

- HIPAA requires payers to implement **electronic transaction standards** (or transactions rule), which is a uniform language for electronic data interchange.
- **Electronic data interchange (EDI)** is the process of sending data from one party to another using computer linkages. The CMS Standard EDI Enrollment Form must be completed prior to submitting electronic media claims (EMC) to Medicare. The agreement must be executed by each provider of healthcare services, physician, or supplier that intends to submit EMC.

# Electronic Healthcare Transactions

**EXAMPLE:** Healthcare providers submit electronic claims data to payers on computer tape, diskette, or by computer modem or fax. The payer receives the claim, processes the data, and sends the provider the results of processing electronic claims (an electronic remittance advice).



# Privacy and Security Standards

- Any information communicated by a patient to a healthcare provider is considered **privileged communication**, and HIPAA provisions address the privacy and security of protected health information.
- **Protected health information (PHI)** is information that is identifiable to an individual (individual identifiers) such as name, address, telephone numbers, date of birth, Medicaid ID number and other medical record numbers, social security number (SSN), and name of employer.

Chapter  
04

# Privacy and Security Standards

- In most instances, covered entities (providers, payers, and clearinghouses) are required to obtain an **individual's authorization** prior to disclosing the individual's health information, and HIPAA has established specific requirements for an authorization form.
- **Privacy** is the right of individuals to keep their information from being disclosed to others. Once information is disclosed (e.g., for the purpose of obtaining health care), it is essential that confidentiality of the information be maintained.

# Privacy and Security Standards

- **Confidentiality** involves restricting patient information access to those with proper authorization and maintaining the security of patient information.
- **Security** involves the safekeeping of patient information by:
  - Controlling access to hard copy and computerized records (e.g., implementing password protection for computer-based patient records).
  - Protecting patient information from alteration, destruction, tampering, or loss (e.g., establishing office policies).

## Privacy and Security Standards

- Providing employee training in confidentiality of patient information (e.g., conducting annual in-service education programs).
- Requiring employees to sign a confidentiality statement that details the consequences of not maintaining patient confidentiality (e.g., employee termination).

# Privacy and Security Standards

- **Breach of confidentiality**, often unintentional, involves the unauthorized release of patient information to a third party, as in the following examples:
  - Discussing patient information in public places (e.g., elevators).
  - Leaving patient information unattended (e.g., computer screen display).
  - Communicating patient information to family members without the patient's consent.
  - Publicly announcing patient information in a waiting room or registration area.
  - Accessing patient information without a job-related reason.

# Privacy and Security Standards

- **NOTE:** Healthcare providers are required to notify patients when the security of their protected health information has been breached. (A breach occurs when protected health information (PHI) is acquired, accessed, used, or disclosed in a way that poses “significant risk of financial, reputational, or other harm to the individual.” )
- Providers must notify individuals to whom the PHI pertains within 60 days after discovery of the breach.
- Providers also have a duty to notify the media of any breach that affects more than 500 individuals residing in one state or jurisdiction.

# Privacy and Security Standards

- Although HIPAA privacy regulations do not require providers to obtain patient authorization for the release of healthcare information to payers for processing insurance claims, many providers continue to obtain patient authorization.
- The best practice is to advise patients that they have the right to restrict the release of their healthcare information (e.g., patient writes a letter informing the provider that medical records are not to be released to insurance companies).

# Privacy and Security Standards

- When a patient restricts the release of healthcare information, the provider should obtain the patient's signature on a consent form accepting financial responsibility for the cost of treatment.
- An insurance company that is prohibited from reviewing patient records will probably refuse to reimburse the provider for a submitted claim. The signed consent form accepting financial responsibility allows the provider to collect payment from the patient.
- If patient authorization is obtained, be sure the patient has signed an “authorization for release of medical information” statement before completing the claim.

# Privacy and Security Standards

- **NOTE:** Although security and privacy are linked, be sure you do not confuse the purpose of each rule.
- The **security rule** defines administrative, physical, and technical safeguards to protect the availability, confidentiality, and integrity of electronic protected health information (PHI).
- The **privacy rule** establishes standards for how PHI should be controlled, by indicating authorized uses (e.g., continuity of care) and disclosures (e.g., third-party reimbursement) and patients' rights with respect to their health information (e.g., patient access).

# Retention of Records

**EXAMPLE 2:** Dr. Smith practices in Delaware (DE), which mandates that medical records be retained for 5 years. Because the HIPAA mandate is stricter than DE state law, Dr. Smith must retain patient records for a period of 6 years. For any patient who has died, Dr. Smith must retain the record for a period of 2 years after the date of death.

# Key Takeaways

1. Federal and state statutes are laws passed by legislative bodies and implemented as regulations.
2. The Federal Register is a legal newspaper published every business day by the federal government.
3. Record retention is the storage of documentation for an established period of time, usually mandated by federal and/or state law.
4. The Health Insurance Portability and Accountability Act (HIPAA) includes the following provisions: fraud and abuse guidelines, electronic health information transaction standards, and privacy and security standards for health information.



Thank You