2020

Medical Billing Training: Certified Professional Biller (CPB™)

Disclaimer

This curriculum was current when it was published. Every reasonable effort has been made to assure the accuracy of the information within these pages. The ultimate responsibility lies with readers to ensure they are using the codes and following applicable guidelines correctly. AAPC employees, agents, and staff make no representation, warranty, or guarantee that this compilation of information is error-free, and will bear no responsibility or liability for the results or consequences of the use of this course. This guide is a general summary that explains guidelines and principles in profitable, efficient healthcare organizations

US Government Rights

This product includes CPT®, which is commercial technical data and/or computer data bases and/or commercial computer software and/or commercial computer software documentation, as applicable, which was developed exclusively at private expense by the American Medical Association, 515 North State Street, Chicago, Illinois, 60610. U.S. government rights to use, modify, reproduce, release, perform, display, or disclose these technical data and/or computer data bases and/or computer software and/or computer software documentation are subject to the limited rights restrictions of DFARS 252.227-7015(b)(2) (November 1995), as applicable, for U.S. Department of Defense procurements and the limited rights restrictions of FAR 52.227-14 (June 1987) and/or subject to the restricted rights provision of FAR 52.227-14 (June 1987) and FAR 52.227-19 (June 1987), as applicable, and any applicable agency FAR Supplements, for non-Department of Defense Federal procurements.

AMA Disclaimer

Fee schedules, relative value units, conversion factors and/or related components are not assigned by the AMA, are not part of CPT®, and the AMA is not recommending their use. The AMA does not directly or indirectly practice medicine or dispense medical services. The AMA assumes no liability for data contained or not contained herein.

Clinical Examples Used in this Book

AAPC believes it is important in training and testing to reflect as accurate a setting as possible to students and examinees. All examples and case studies used in our study guides and exams are actual, redacted office visit and procedure notes donated by AAPC members. To preserve the real-world quality of these notes, we have not re-written or edited the notes to the stringent grammatical or stylistic standards found in the text of our products. Some minor changes have been made for clarity or to correct spelling errors originally in the notes. The notes otherwise appear as one would find them in a coding setting.

2233 South Presidents Dr., Suites F-C, Salt Lake City, UT 84120-7240
800-626-2633, Fax 801-236-2258, www.aapc.com
Updated 10212019. All rights reserved.

ISBN 978-1-626888-005

Chapter 1

Introduction to Healthcare

Introduction

AAPC would like to introduce this curriculum that will benefit medical billers and other medical professionals to further their understanding of the business side of medicine. This material was developed to instruct billers and other medical professionals and help them prepare for the Certified Professional Biller exam necessary to obtain the CPB™ credential.

AAPC has prepared this curriculum aimed at providing the most up-to-date information relating to billing, including HIPAA, consumer driven health plans, ICD-10-CM, CPT®, accounts receivable (A/R), and health plans (governmental and commercial).

The objectives for this chapter include:

- Understand a background in healthcare
- Provide an overview of HIPAA including privacy standards, HITECH security rules, and transaction and code set standards
- Recognize standards for Conditions of Participation (CoP)
- Recognize the difference between fraud and abuse
- Identify how the False Claims Act (FCA) affects billing practices
- Review federal regulations including Stark Law, Anti-Kickback, and Healthcare Fraud Statute
- Understand how the Truth in Lending Act affects collection efforts
- Summarize the Quality Payment Program (QPP)

Background of Healthcare

The business of medicine is highly complex, ever changing, and tightly regulated. Healthcare providers are subject to many guidelines and requirements, as implemented by insurers and government agencies. These rules cover a wide range of issues, from how providers must handle medical records, to the documented diagnoses or clinical indications a patient must demonstrate if an insurer is to pay for a procedure, and regulations for payment timelines and refunds.

Until the 1940s, healthcare insurance was not commonplace for Americans. During World War II, wage and price controls were placed on employers by the 1942 Stabilization Act. Congress limited the wages that could be offered but allowed the adoption of employee insurance plans. The 1954 Internal Revenue Code stated employer contributions to employee health plans were exempt from employee taxable income, making the demand for health insurance even more appealing.

Medicare was passed into law on July 30, 1965 by President Lyndon B. Johnson under title XVIII of the Social Security Act. Beneficiaries were able to sign up for the program on July 1, 1966. U.S. citizens were automatically enrolled in Part A Medicare at age 65, which covered hospital stays, and had an option to choose to enroll in Part B Medicare, which covered physician services.

The Health Maintenance Organization (HMO) Act of 1973 (P. L. 93-222) was proposed under the Nixon Administration to try to help control healthcare costs. It authorized $375 million to assist in establishing and expanding HMOs. The Act also overrode state laws that prohibited the establishment of prepaid health plans and required employers with 25 or more employees to offer an HMO option if they furnished healthcare coverage to their employees. According to the Rand Corporation, HMO enrollment went from three million in 1970 to over 80 million in 1999, representing a 12 percent increase every year.

Preferred Provider Organizations (PPO) then emerged. A PPO is within the framework of managed care health insurance. PPOs set up a group of doctors, hospitals, and other healthcare providers to create a network and negotiate predetermined fees with a given carrier. PPOs offer members more options in that they do not have to maintain a primary care physician, nor does it require referrals.

The addition of these and other types of health plans have led to a high level of complexity in the business of medicine. Hospitals, clinics, and private physician practices all have to contend with many issues in order to stay in business. This has led to the expansion in the healthcare field of medical professionals with the skill sets necessary to keep the business side running smoothly.

Healthcare Regulations

Healthcare regulations are not always definitive and may vary by payer, geographic area, and the setting in which patient care is provided. To be effective, the biller must distinguish and comprehend the precise regulatory requirements that apply in a particular circumstance. The healthcare regulations that affect medical billing will be reviewed in this chapter.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted on August 21, 1996. HIPAA was originally passed to provide rights and protections for participants and beneficiaries of group health plans. Under this law, exclusions for pre-existing conditions were limited, and discrimination against employees and dependents based on their health status were prohibited. HIPAA also established the Healthcare Fraud and Abuse Control Program (HCFAC), a far-reaching program to combat fraud and abuse in healthcare including both public and private health plans. HCFAC is designed to coordinate federal, state, and local law enforcement activities with respect to healthcare fraud and abuse. The US Department of Health and Human Services (HHS) and Department of Justice (DOJ) are required to provide an annual report detailing the efforts and recoveries made by the HCFAC program.

HIPAA Administrative Simplification provisions required that sections of the law be publicized to explain the standards for the electronic exchange, privacy, and security of health information. Congress did not enact privacy legislation within the specified time governed by HIPAA. The HHS then developed a proposed rule, which was published and released in final form on August 14, 2002.

Privacy Rule

The Privacy Rule standards address how an individual's protected health information (PHI) may be used. PHI is "individually identifiable health information" that includes many common identifiers, such as demographic data, name, address, birth date, and social security number. It also includes information that relates to an individual's past, present, or future physical or mental health or condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual, which reasonably may be used to identify an individual.

To fully understand protected health information, let's look at the definitions of health information and individually identifiable health information. For information to be regulated by the Privacy Rule, the information would need to fall within both definitions.

HEALTH INFORMATION

Section 1171 of Part C of Subtitle F of Public Law 104-191

(4) HEALTH INFORMATION. The term health information means any information, whether oral or recorded in any form or medium, that:

(A) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Section 1171 of Part C of Subtitle F of Public Law 104-191

(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION–The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that:

(A) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual

The purpose of the Privacy Rule is to protect individual privacy while promoting high quality healthcare and public health and well-being. All covered entities are required to follow the Privacy Rule. Covered entities are defined as health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in an electronic format.

- **Health Plan** covered entities are organizations that pay providers on behalf of an individual receiving medical care. These plans include health, dental, vision, and prescription drug insurers (for example, Health Maintenance Organizations (HMOs), Medicare, Medicaid, and employer, government, and church-sponsored group health plans). There are exceptions, such as an employer who solely establishes and maintains the plan with fewer than 50 participants is exempt. Two types of government-funded programs are exempt; food stamps and community health centers. Insurers providing only workers' compensation, automobile insurance, and property and casualty insurance are not considered to be health plans.

- **Healthcare providers** who electronically transmit health information through certain transactions are covered entities. Some examples of transactions that may be submitted electronically are claim forms, inquiries about eligibility of benefits, and requests for authorization of referrals. Simply using electronic technology, such as sending emails, does not mean a healthcare provider is a covered entity; the transmission must be in connection with a standard transaction. The rule applies to all healthcare providers, regardless of whether they transmit the transactions directly, or use a billing service or other third party to transmit on their behalf.
- **Healthcare clearinghouses** include billing services, re-pricing companies, and community health management information systems that process nonstandard information, received from another entity, into a standard (or vice versa).

Business associates perform certain functions or activities, which involve the use or disclosure of individually identifiable health information, on behalf of another person or organization. These services include claims processing or administration, data analysis, utilization review, billing, benefit management, and re-pricing. Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. To be considered a business associate, the persons or organizations would involve the use or disclosure of PHI between the two parties.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, also specifies that an organization that provides data transmission of PHI to a covered entity and that requires access to PHI routinely, such as a Health Information Exchange Organization (HIEO), will be treated as a business associate. A contract is required between business associates to impose specified written safeguards on the individually identifiable health information used or disclosed by the business associate. If a covered entity identifies a material breach or violation of the contract or agreement, reasonable steps must be taken to cure the breach or end the violation. If that is not possible, the contract must be terminated, and the problem reported to the HHS Office for Civil Rights (OCR).

The Privacy Rule includes exceptions to the business associate standard, which do not require a covered entity to have a written agreement in place prior to disclosing PHI. Examples include:

- Disclosures by a covered entity to a healthcare provider for treatment of the individual, such as:
  - A healthcare provider scheduling a surgery at a hospital for the patient.
  - A healthcare provider sending specimens to a hospital lab or reference lab for analysis
  - A hospital transferring a patient to a nursing home for continued care
- Disclosures to a health plan sponsor, such as an employer, by a group health plan that provides the health insurance benefits or coverage for the group health plan.
- The collection and sharing of PHI by a health plan that is a public benefits program, such as Medicare.

The Privacy Rule allows for de-identification of health information. To de-identify health information, any information that could help identify the individual is removed. This includes the following information as it relates to the individual patient, relatives, employers, or household members:

- Names
- Demographic information (geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes)
- Dates directly related to the individual (date of birth, admission and discharge dates, death date, etc.)
- Telephone numbers, fax numbers, and email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers (health plan ID, health plan subscriber number)
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers (for example, implants)
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voiceprints
- Full-face photographs and any comparable images
- Any other unique identifying number, characteristic, or code

De-identification guidance can be found on the HHS website: https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#rationale.

There are no restrictions on the use of de-identified health information. When the PHI is removed, a reasonable basis does not exist to identify an individual.

BILLING TIP

De-identified health information may also be referred to as redacted. Redacted means to obscure or remove information from a document prior to release.

A covered entity may not use or disclose PHI unless the Privacy Rule permits it, or as the individual authorizes in writing. The rule requires that a covered entity must disclose PHI to an individual when he or she requests his or her own information or to HHS when it is investigating for compliance, review, or enforcement action.

Permitted uses and disclosures of PHI allow a covered entity to use and disclose certain information without an individual's authorization in the following situations:

1. Release of records to the individual who is the subject of the information. A patient has the right to inspect, review, and receive a copy of their medical records and billing records. A provider may charge a reasonable cost for copying and mailing the records.

2. By a covered entity for treatment, payment, and healthcare operation activities.

   Treatment is the provision, coordination, or management of healthcare services among healthcare providers. This includes consultation between healthcare providers regarding a patient, or the referral of a patient from one healthcare provider to another.

   Payment includes a variety of activities for a provider to be reimbursed for their services and for a health plan to obtain premiums and provide benefits. Examples of payment activities include determining eligibility and benefits, billing and collection activities, reviewing healthcare services for medical necessity, coverage, justification of charges, and adjudication of claims.

   Operation includes administrative, financial, legal, and quality improvement activities necessary to run a business and support the core functions of treatment and payment. Examples of operations include quality assessment and improvement activities, evaluating provider and health plan performance, conducting medical review, legal, and auditing services including fraud and abuse detection and compliance programs.

3. The individual may grant informal permission by being asked outright, giving them the opportunity to agree or object in circumstances where the individual is not capable of providing his or her signature. Covered entities are expected to use their judgment in situations where the patient is incapacitated, or the covered entity is not available to provide the care that is in the best interest of the patient.

   For example, this provision allows for a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient, or for notifying family members of the individual's location, general condition, or death.

4. Incidental use and disclosure is permitted if the covered entity has reasonable safeguards in place to ensure that the information being shared is limited to the "minimum necessary," as required by the Privacy Rule. According to the OCR, an incidental use or disclosure is "a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs because of another use or disclosure that is permitted by the rule."

CASE EXAMPLE: ACCESS TO MEDICAL RECORDS

Private Practice Revises Process to Provide Access to Records

Covered Entity: Private Practices

Issue: Access

A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. OCR's investigation determined that the private practice had relied on state regulations that permit a covered entity to provide a summary of the record. OCR provided technical assistance to the covered entity, explaining that the Privacy Rule permits a covered entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the covered entity to revise its policy. In addition, the covered entity forwarded the complainant a complete copy of the medical record.

Source: https://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case14

Minimum Necessary

The Minimum Necessary Standard is a key protection of HIPAA Privacy Rule. The rule requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. A covered entity is required to develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary.

When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a purpose, unless it can specifically justify the whole record as the amount reasonably needed for that purpose.

For example, when documentation is requested by a payer for processing of a claim, only documentation pertinent to that service should be sent to the payer. Sending the entire medical record would be a violation of minimum necessary.

BILLING TIP

Medical billers often receive requests for medical records for processing claims. A medical biller should respond to the request for records by providing only the dates of service requested, or the minimum necessary.

CASE EXAMPLE: MINIMUM NECESSARY

Hospital Implements New Minimum Necessary Polices for Telephone Messages

Covered Entity: General Hospital

Issue: Minimum Necessary; Confidential Communications

A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. One addressed the issue of minimum necessary information in telephone message content. Employees were trained to provide only the minimum necessary information in messages and were given specific direction as to what information could be left in a message. Employees also were trained to review registration information for patient contact directives regarding leaving messages. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.

Source: https://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case26

To strike a balance between the individual interest and public interest for specific PHI, the Privacy Rule permits use and disclosure of this information without an individual's authorization or permission through public interest and benefit activities. There are 12 national priority purposes:

1. Required by law

   PHI may be disclosed by a covered entity when required by law. This includes by statute, regulation, or court orders.

2. Public health activities

   PHI may be released to public health authorities who are legally authorized to receive reports to prevent and control disease, injury, or disability. This may also include releasing information for the Food & Drug Administration (FDA) regulated products and for individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law.

3. Victims of abuse, neglect or domestic violence

   A provider may disclose PHI to report known or suspected child abuse or neglect to a public health authority such as the social services department of a local government.

4. Health oversight activities

   PHI may be disclosed to health oversight agencies for legally authorized health oversight activities. Audits and investigations for oversight of the healthcare system and government benefit programs such as Medicare and Medicaid are included in these oversight activities.

5. Judicial and administrative proceedings

   Court orders and administrative tribunals allow the release of PHI in a judicial or administrative proceeding. When a provider receives a subpoena, they may release the PHI if notice is given to the individual or a protective order is provided.

6. Law enforcement purposes

   PHI may be released for law enforcement purposes:

   - as required by law (court order, court ordered warrants, etc.)
   - to identify or locate a suspect, fugitive, material witness, or missing person
   - for information about a victim or suspected victim of a crime
   - about a death when there is suspicion that criminal activity caused death

- as evidence of a crime that occurred on the covered entity's premises
- in a medical emergency, not occurring on the premises, to inform law enforcement of details about the crime such as the nature of the crime, location, etc.

7. Decedents

   PHI may be released to coroners, medical examiners, and funeral directors.

8. Cadaveric organ, eye, or tissue donation

   Facilitation of donation and transplantation of cadaveric organs, eye, or tissue can be released by a covered entity.

9. Research

   Information used in research can be de-identified. If the information is de-identified, it is not covered by the Privacy Rule. Information that is not de-identified may be used without individual authorization for research in limited circumstances.

10. Serious threat to health or safety

    PHI may be released to prevent or lessen a serious and imminent threat to a person or the public.

11. Essential government functions

    Some activities included in essential government functions include protecting the health and safety of inmates or employees in a correctional institution, assuring proper execution of a military mission, etc.

12. Workers' compensation

    The Privacy Rule does not apply to workers' compensation insurers, workers' compensation administrative agencies, or employers. Covered entities may disclose PHI when required by workers' compensation laws or to obtain payment. The Minimum Necessary provision must be taken into consideration when determining what to disclose.

BILLING TIP

A covered entity may disclose PHI required by a court order or administrative tribunal. A subpoena issued by a court clerk or an attorney in a case (someone other than a judge) is not synonymous with a court order. When a subpoena is issued, it should be accompanied by a court order to release the records. Only the records specified in the order may be disclosed. When the subpoena is not accompanied by a court order, the covered entity must make a reasonable effort to:

1. Notify the person who is the subject of the PHI about the request, giving them a chance to object to the disclosure; or
2. Seek a qualified protective order for the information from the court.

Source: https://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/courtorders.html

A limited data set is PHI from which certain specified direct identifiers have been removed. Limited data sets may be used for research, healthcare operations, and public health purposes, as long as there is an agreement with promised safeguards in place for the PHI.

A privacy practice notice must be provided by each covered entity. The notice must clearly explain the covered entity's obligation to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The covered entity should also inform the patient of his or her individual rights, and the steps to follow (including a point of contact for further information) if an individual feels his or her privacy rights have been violated.

Covered entities are required to supply a notice to anyone upon request, whether direct or indirect treatment was provided. In addition, covered entities also need to make its privacy notice available electronically on any website it maintains for customer service or benefits information.

A healthcare provider must make a good faith effort to obtain written acknowledgement from patients that the patients have received the privacy practices notice. Most covered entities ask for signatures from individuals, indicating that the individual was provided a copy of the notice. Receipt of acknowledgement is relieved in emergent situations.

In most cases, individuals have the right to review and obtain copies of their PHI. Areas excluded from the rights of access are: psychotherapy notes, information related to legal proceedings, and certain lab results or information held by research laboratories. Covered entities may charge a reasonable fee for providing such information.

There is some flexibility and scalability built into the rule to allow analysis of each entity's needs, and to implement the required rules appropriately. The administrative requirements that must be followed are:

- All covered entities must have written privacy policies that comply with the Privacy Rule.

- A privacy official must be designated to be responsible for developing and implementing privacy policies and procedures, and be the contact person for individuals with questions or concerns regarding the privacy practices.
- All members of a covered entity's workforce (employees, volunteers, and trainees) must be trained on the covered entity's privacy policies. Appropriate sanctions must be applied to a workforce member who violates any area of the privacy rules.
- Covered entities are required to mitigate any harmful effect that may have been caused by inappropriate use or disclosure of PHI that was caused by its workforce or business associates.
- Procedures must be in place to allow an individual to complain about a covered entity's compliance with their privacy policies.
- A covered entity may not retaliate against a person for exercising his or her rights provided by the Privacy Rule or require an individual to waive any right to obtain healthcare services.
- Privacy policies must be maintained by covered entities for six years, after the later of the date of their creation, or last effective date.
- Fully insured group health plans have only two obligations: (1) refrain from retaliatory acts and waiver of individual rights, and (2) to provide documentation for the disclosure of PHI through documentation.

Security Rule

The HIPAA Security Rule was established by the HIPAA Administrative Simplification Regulations to establish national standards to protect and secure patient data that is stored or transmitted electronically. It requires that appropriate administrative, physical, and technical safeguards are in place to ensure confidentiality and security of patient health information. This regulation is to be adopted by health plans, healthcare clearinghouses, and covered healthcare providers. The Security Rule also requires policies and procedures be implemented to comply with the Security Rule. The policies and procedures are required to be maintained for six years from the date of creation or the date when last in effect, whichever is later.

A breach notification rule requires HIPAA covered entities to provide notification in the event of an unsecured breach of patient health information. A breach occurs when an impermissible release of, or disclosure of information is discovered. A breach can occur by many methods, such as discs, USB, or thumb drives being misplaced or lost, paper or hard copies not being properly disposed of, backup files not being secure, and/or information being sent to unprotected portable devices.

CASE: BREACH

A hospital system took custody of medical records belonging to a retiring physician with the intent of assisting in the transition of care for the 5,000-8,000 patients and considered the possibility of purchasing the physician's practice. Hospital staff returned the records to the physician's home, in his absence, and left 70 boxes of records on the driveway unattended. Because the hospital was a covered entity with custody of the records, they were responsible to safeguard the protected health information in its custody. The settlement of $800,000 also stated that a corrective action plan be put in place to update policies and procedures, and to educate staff.

BILLING TIP

The biller should be aware of the Security Rule and of the office policy in case of a breach of PHI. Physician offices are responsible for controlling the way in which patient's PHI is used, stored, and disclosed.

Transaction and Code Sets

Transactions occur through electronic exchanges, which allow information to be transferred between two parties for specific purposes. A healthcare provider will send a claim to a health plan to request payment for the medical services he or she provides. Under HIPAA, provisions were included for Administrative Simplification that mandated HHS to adopt national standards for electronic healthcare transactions and code sets. The eight standard transactions for Electronic Data Interchange (EDI) adopted under HIPAA are:

1. Claims and encounter information;
2. Healthcare payment and remittance advice;
3. Healthcare claims status;
4. Eligibility for a health plan;
5. Enrollment and disenrollment in a health plan;
6. Referrals and authorizations;
7. Coordination of benefits; and
8. Health plan premium payments.

If a covered entity under HIPAA conducts any of the above transactions electronically, they must use the adopted standard- ASC X12 Version 5010 or NCPDP (used for certain pharmacy transactions) for each transaction.

An additional rule was also adopted to standardize the code sets for diagnoses and procedures to be used in all transactions. The code sets adopted are:

- Healthcare Common Procedure Coding System (HCPCS): code set established by CMS to represent services not covered by CPT®.
- Current Procedure Terminology (CPT®): code set maintained by the American Medical Association to describe medical procedures and physician services.
- International Classification of Diseases, 10th Revision, Clinical Modification, (ICD-10-CM) contains the diagnosis codes and is maintained by the National Center for Health Statistics, Centers for Disease Control. ICD-10-PCS contains procedures and is maintained by CMS and is used to report procedures for inpatient hospital services.
- National Drug Codes (NDC): code set that identifies vendor, product, and package size of all drugs and biologicals recognized by the FDA, maintained by HHS.
- Current Dental Terminology (CDT®): code set for dental services maintained by the American Dental Association (ADA).
- Place of Service Codes: two-digit codes placed on all healthcare professional claims that denote the setting in which the service was provided. The codes are maintained by CMS.

In addition to the standardization of the codes used to request payment for medical services, a unique identifier for employers and providers must be used on all transactions.

Section Review 1.1

1. HIPAA of 1996 includes a Security Rule that is established to provide what national standards for protecting and transmitting patient data. Which of the following is NOT true?

   A. The Security rule applies to healthcare providers, health plans, and any covered entity involved in the care of the patient.

   B. The Security Rule applies only to the entity that initiates the release of protected health information.

   C. Standards for storing and transmitting patient data in electronic form include portable electronic devices.

   D. The Security Rule states that safeguards must be in place to prevent unsecured release of information.

2. Eight standard transactions were adopted for Electronic Data Interchange (EDI) under HIPAA. Which of the following is NOT included as a standard transaction?

   A. Payment and remittance advice

   B. Eligibility in a health plan

   C. Coordination of benefits

   D. Physician unique identifier number

3. A claim is received by a payer that subsequently requests the medical records for the date of service on the claim. What procedure should be followed by the practice?

   A. Only the date of service on the claim should be sent to the payer. The records can be sent as part of HIPAA based on treatment, payment, and operations (TPO).

   B. The records for the claim can be sent after authorization is received from the patient.

   C. The entire patient record should be sent as part of HIPAA based on treatment, payment, and operations.

   D. The payer is required to provide authorization signed from the patient prior to requesting the medical records.

4. HIPAA requires that privacy practice notices be provided in several circumstances. Which one of the following is NOT required?

   A. Must be available on any website the practice maintains
   B. Must be provided upon request
   C. Must be presented to all patients
   D. Must be placed into the patient's file

5. When a subpoena is received by the practice for medical records, in what circumstances may the records be released according to the HIPAA Privacy Rule?

   A. The subpoena allows for the release of the medical records.
   B. The subpoena is accompanied by a court order or the patient is notified and given a chance to object.
   C. The individual must sign an authorization for release of the information.
   D. Records cannot be released under any circumstance based on a subpoena.

Conditions of Participation (CoP)

CMS and other health plans have conditions that healthcare organizations must meet to participate with the plan or program. CoPs are designed to protect patient health and safety, and to ensure quality of care. These apply to entities such as: ambulatory surgical centers, hospitals, hospices, clinics, psychiatric hospitals, long term care facilities, and transplant centers.

Records Retention

Medical records need to be retained for many reasons:

- Provide continuity of care
- Support services with health plan claim inquiries
- Assist in audits
- Meet legal requirements
- Provide defense against complaints and negligence claims
- Required as a condition of participation in a health plan

Many things need to be taken into consideration when deciding on a time frame for medical record retention. A single standardized record retention schedule does not exist.

CMS COPS CONTAIN INFORMATION ON RECORDS RETENTION AS SEEN BELOW

§482.24 Condition of participation: Medical record services.

The hospital must have a medical record service that has administrative responsibility for medical records. A medical record must be maintained for every individual evaluated or treated in the hospital.

(a) *Standard: Organization and staffing*– The organization of the medical record service must be appropriate to the scope and complexity of the services performed. The hospital must employ adequate personnel to ensure prompt completion, filing, and retrieval of records.

(b) *Standard: Form and retention of record*– The hospital must maintain a medical record for each inpatient and outpatient. Medical records must be accurately written, promptly completed, properly filed and retained, and accessible. The hospital must use a system of author identification and record maintenance that ensures the integrity of the authentication and protects the security of all record entries.

(1) Medical records must be retained in their original or legally reproduced form for a period of at least 5 years.

CMS requirements for records are as follows:

- Medical records must be retained in their original or legally reproduced form for a period of at least five years.
- For providers submitting cost reports to be retained in their original or legally reproduced form for a period of at least five years after the closure of the cost report.
- For Managed care program, providers should retain records for 10 years.

Medical records may be retained in any media format: paper, electronic, or digital. The only requirement is that it be either in its original form or in a legally reproduced form.

The HIPAA Privacy Rule does not include medical record retention requirements. It does, however, require 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. The administrative simplification rules under HIPAA require a covered entity to retain required documentation for six years form the date of its creation or the date when it was last in effect, whichever is later. HIPAA requirements take precedence over state laws if they require shorter periods of retention. State laws on records retention vary from type of provider (medical doctor versus hospital) and age of patient (adult versus minor).

The federal False Claims Act (31 USC § 3729) allows for claims to be brought up to seven years after the incident but has been extended to 10 years in some cases. This should be kept in mind.

Fraud vs. Abuse

A CPB™ must be educated on the federal departments and regulations regarding fraud and abuse. During the first half of FY 2017, OIG reported expected investigative recoveries of over $2.04 billion. Commercial health plans are also recouping money, and many have their own fraud and abuse departments.

CMS defines fraud as making false statements or misrepresenting facts to obtain an undeserved benefit or payment from a federal healthcare program. CMS defines abuse as an action that results in unnecessary costs to a federal healthcare program, either directly or indirectly.

CMS examples of fraud:

- Billing for services and/or supplies that you know were not furnished or provided
- Altering claim forms and/or receipts to receive a higher payment amount
- Billing a Medicare patient above the allowed amount for services
- Billing for services at a higher level than provided or necessary
- Misrepresenting the diagnosis to justify payment
- Falsifying documentation

CMS examples of abuse:

- Misusing codes on a claim
- Charging excessively for services or supplies
- Billing for services that were not medically necessary
- Failure to maintain adequate medical or financial records
- Improper billing practices
- Billing Medicare patients a higher fee schedule than non-Medicare patients

BILLING TIP

Medical billers should have knowledge of the federal regulations and understand the penalties associated with the regulations. Understanding the depth of fraud and abuse can help a medical biller understand the impact of the billing department in keeping a practice from abuse.

Fraud and abuse carry stiff penalties under 42 USC § 1320a-7a of the United States Code. Civil monetary penalties (CMPs) may be imposed to varying amounts, depending on the type of violation. These penalties range from $10,000 to $50,000 (before inflation adjustment) per violation and can include up to three times the amount claimed for each item or service, or up to three times the amount of remuneration offered, paid, solicited, or received, whether a portion of such remuneration was offered, paid, solicited, or received for a lawful purpose. On top of all that, exclusion from participation in the federal healthcare programs and state healthcare programs may be imposed, along with criminal penalties of fines, imprisonment, or both.

The Department of Justice (DOJ), the Department of Health & Human Services Office of Inspector General (OIG), and the Centers for Medicare & Medicaid Services (CMS) are the government agencies that enforce the federal fraud and abuse laws.

False Claims Act (FCA)

The False Claim Act protects the government from being overcharged or sold substandard goods or services.

The False Claims Act (31 U.S.C. §§ 3729–3733) states that any person is liable under the FCA if he or she:

(A) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;

(B) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;

(C) Conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G);

(D) Has possession, custody, or control of property or money used, or to be used, by the government and knowingly delivers, or causes to be delivered, less than all of that money or property;

(E) Is authorized to make or deliver a document certifying receipt of property used, or to be used, by the government and, intending to defraud the government, makes or delivers the receipt without

completely knowing that the information on the receipt is true;

(F) Knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the government, or a member of the Armed Forces, who lawfully may not sell or pledge property; or

(G) Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government.

Relative to healthcare services, examples of fraud or misconduct subject to the False Claims Act include:

- Falsifying a medical chart notation
- Submitting claims for services not performed, not requested, or unnecessary
- Submitting claims for expired drugs
- Upcoding and/or unbundling services
- Submitting claims for physician services performed by a non-physician provider (NPP) without regard to Incident-to guidelines

CASE EXAMPLE

A physician billed for urine drug screening in the office setting and submitted claims for Medicare patients using low to moderate complexity urine drug tests that exceeded the number of units allowed by Medicare. The office used an inappropriate code that would bypass the system and allow for reimbursement of a test that would have otherwise been denied. The code reported by the office was for a higher complexity drug screen than was performed. The physician was ordered to repay $334,538.90.

Failure to Return Overpayments

The final section (a.1.G), above, is known as the "reverse false claims" section. It provides liability where a person acts improperly to *avoid* paying money owed to the government. In the FCA (31 USC §3729 (b) (3) (2010)), obligation is defined as "an established duty, whether fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment."

Congress also amended the Medicare and Medicaid program integrity provisions to identify the extent of a provider's obligations when an overpayment is identified. It states that a provider must report and return an overpayment to the Secretary of HHS, the state, an intermediary, a carrier, or a contractor, as appropriate, by the later of 60 days from the date when the overpayment was "identified" or the date "any corresponding cost report is due." The provider must notify the party to whom the overpayment was returned, in writing, of the reason of the overpayment.

Deliberate Ignorance of the Truth

The FCA is violated by submitting a false claim *with knowledge that it is false*; however, the Act states that a violation may occur *even if there no intent to defraud*. The FCA defines the terms as follows:

The terms "knowing" and "knowingly"—

(A) mean that a person, with respect to information—

(i) has actual knowledge of the information;

(ii) acts in deliberate ignorance of the truth or falsity of the information; or

(iii) acts in reckless disregard of the truth or falsity of the information; and

(B) require no proof of specific intent to defraud.

According to United States legal definitions, deliberate ignorance of the truth means intentionally ignoring a fact when one has every reason to believe about its existence. When knowledge of existence of that fact is an essential part of an offense, such knowledge may be established if the person is aware of a high probability of its existence.

Current penalties are $5,500 to $11,000 (before annual inflation adjustment) per claim. The person in violation will also be liable for the costs of the civil action brought to recover any such penalty or damages. The FCA allows for reduced penalties (mitigation) if the person committing the violation self-discloses and meets other requirements. This amount is occasionally increased based on the Federal Civil Penalties Inflation Adjustment Act (FCPIA). CMPs for False Claims Act violations are $11,463 to $22,927 per claim for 2019.

Qui Tam

The *Qui Tam* or "whistleblower" provision is described in §3730. If an individual knows of a violation of the FCA, he or she may bring a civil action on behalf of him or herself *and* on behalf of the U.S. government (such an individual is called a relator). If the government intervenes, it has the primary responsibility for prosecuting the Qui Tam action. The relator may be awarded 15–25 percent of the dollar amount recovered

through the Qui Tam action, depending on the extent to which the relator contributed to the prosecution. If the government declines to intervene in the action, the relator's share is increased to 25 to 30 percent. Since 1986, recoveries in Qui Tam actions have exceeded $18 billion.

Common defendants in Qui Tam actions are government contractors and subcontractors; colleges and universities; medical care providers, such as physicians, clinics, and hospitals; health maintenance organizations (HMOs); and federal grantees.

The statute seeks to protect possible relators who come forward with information of wrongdoing. §3730 h.1, states that a relator shall be entitled to all relief necessary to make him or her whole if he or she is discharged, demoted, suspended, threatened, harassed, or in any manner discriminated against in the terms and conditions of employment because of lawful acts done by the relator in furtherance of the efforts to stop violations.

CASE EXAMPLE

A hospital and cardiology practice agreed to pay $4 million to settle a lawsuit alleging cardiology procedures were performed on patients that were not medically necessary based on Medicare guidelines. These services were billed to Medicare and Medicaid. The civil suit was brought by a whistleblower who worked as a cardiologist.

Stark Law

The Stark Act is an amendment to the Social Security Act that prohibits physicians from "self-referral" when sending patients elsewhere for certain services. The Stark Law prohibits a physician from making a referral for certain designated health services (DHS) to an entity in which the physician (or an immediate member of his family) has an ownership/investment interest or with which he or she has a compensation arrangement, unless an exception applies. Self-referral of Medicare and Medicaid patients to a facility in which the physician has a vested interest can be considered a conflict of interest and is meant as method of controlling over-utilization of services.

One exception allows for a physician that is a member of a group practice to refer a patient for imaging (CT, MRI, PET) within the group practice without violating Stark. A physician referring a patient within the group practice must provide the patient, at the time of the referral, a list of alternate locations to receive the services or supplies. This exception only applies to those operating within a group practice.

A financial relationship includes direct or indirect ownership of an entity, as well as stock options, partnership interests, and compensation agreements.

The penalties for violation of the Stark Law range from civil penalties of $15,000 (before annual inflation adjustment) for each violation, and up to three times the amount of the improper payment involved in the violation. The violation can also carry the risk for False Claim liability which is discussed later in this chapter.

The Stark Law is similar to the Anti-kickback Law and is governed by Health and Human Services (HHS) (42 USC § 1395nn). It is not the same, however.

Anti-kickback Law

The Anti-Kickback Law (42 United States Code (U.S.C.) Section 1320a-7b(b)) is a federal law that makes it a criminal offense to knowingly or willingly offer, pay, solicit, or receive any remuneration to induce or reward referrals of items or services reimbursable by a federal healthcare program. The Social Security Act of 1972 included the original Anti-kickback legislation. The Health Insurance Portability and Accountability Act of 1996 (See Pub. L. 104-191, 110 Stat. 1936 (1996)) increased the scope of fraud and abuse sanctions.

The Anti-kickback Law states that any items or service that are received by the physician as payment such as cash or gifts, free rent, expensive trips, or meals can be a violation of the Anti-kickback Law and subject to criminal penalties. The penalties for violation of the Anti-kickback statute are fines of up to $25,000 (before annual inflation adjustment) per violation. This can also carry risk for False Claim liability, civil liability, and prison time. One of the most severe penalties associated with the Social Security Act is the ability of the Office of Inspector General (OIG) to exclude an entity or an individual from participation in any and all federal healthcare programs. This includes Medicare, Medicaid, VA programs, and TRICARE. An excluded individual cannot bill for services, provide referrals or prescribe medications or order services for any beneficiary of a federally administered health plan.

EXAMPLE: ANTI-KICKBACK CASES

Case 1:

A recent case alleges that a healthcare system paid cardiologists a percentage of the reimbursement for tests and procedures that the physicians referred to the diagnostic department of the hospital. These physicians were also provided clinical office space for under market value.

Case 2:

In a settled case, a medical device manufacturer paid physicians by giving them free boxes of disposables for exclusive use of their equipment and for recommending the equipment to their colleagues. The medical device manufacturer settled a $1.2 million criminal case and paid $2.5 million in civil penalties.

Criminal Healthcare Fraud Statute

This statute prohibits knowingly or willingly executing of attempting to execute a scheme, such as defrauding any healthcare benefits program (Statute: 18 U.S.C. §§ 1347, 1349).

EXAMPLE: CASE

An owner of a company that provided care to Medicare patients in the beneficiary's home was sentenced to 37 months and ordered to repay $1,223,471. The company hired unlicensed social workers to visit Medicare patients in their home. The services were billed as individual, face-to-face psychotherapy from a licensed clinical social worker when no such services were provided.

Truth in Lending Act (TILA)

The Consumer Credit Protection Act of 1968, also called the Truth in Lending Act, is a federal law that was enacted in 1968. It was designed to protect consumers in their dealings with lenders or creditors.

Finance Charge Assessment

According to the TILA, if the practice regularly extends credit which is payable by agreement in more than four installments, or for which a finance charge is or may be required, they are considered a creditor and are subject to the rules of the Act.

If the practice assesses finance charges on statements, the amount of the finance charge must be disclosed as an annual percentage rate.

If the practice sets up payment plans with patients that extend past four installments, the following information must be disclosed to the patient (as applicable):

- The "cash price" of the service,
- The amount of any down payment,
- The resulting unpaid balance,
- The total amount financed,
- The amount of the finance charge,
- The annual percentage rate of the finance charge,
- The total price to be paid under the credit plan,
- The schedule of payments, including number, amount, and due dates of payments,
- The sum of such scheduled payments, or total of payments, and
- The amount or method of computing the amount of any late payment charges.

If the practice refers patients to an outside finance company for large balances, more extensive disclosure of information to the patient would be required.

There are many regulatory guidelines that affect how a healthcare organization, large or small, may operate their billing practices. For a CPB™ to be effective in the workplace, it is necessary that they have a good understanding of these regulations to keep the organization on a compliant path.

Section Review 1.2

1. A physician received office space at a reduced rate for referring patients to the hospital's outpatient physical therapy center. What Law does this violate?

   A. Anti-kickback Statute
   B. Stark Law
   C. False Claims Act
   D. Truth in Lending Act

2. Federal healthcare plans include what payers?

   A. Blue Cross, Medicare, Humana
   B. Medicare, Medicaid, TRICARE
   C. Medicare, TRICARE, Blue Cross
   D. Humana, VA, TRICARE

3. One of the most severe penalties that can be associated with violations of the Social Security Act is exclusion from federal healthcare plans. Which of the following statements is true of excluded individuals?

   A. Physicians that have been excluded can bill the patient for services but cannot bill federal health plans.
   B. Physicians that have been excluded can refer their patients to other facilities for treatment.
   C. Physicians that have been excluded are prohibited from billing for any services to a federally administered health plan.
   D. Physicians that have been excluded are exempt from billing for services but are allowed to write prescriptions and order tests.

4. A physician billed claims to Medicare and Medicaid for procedures that were not performed on 800 patients resulting in loss of $2.6 million. Is this fraud or abuse?

   A. Fraud; subject to the Anti-kickback Statute
   B. Fraud; subject to the False Claims Act
   C. Abuse; subject only to education of the provider
   D. Abuse; subject to the Stark Law

5. The regulation of finance charges or interest applied to outstanding balances in the medical practice is under what law?

   A. Truth in Lending Act
   B. Criminal Healthcare Act
   C. HIPAA
   D. Conditions of Participation

The Quality Payment Program

In April 2015, Congress passed the Medicare Access and CHIP Reauthorization Act (MACRA), which provided significant changes to the healthcare delivery system. First, MACRA repealed the sustainable growth rate (SGR) formula for physician payment updates in Medicare, preventing scheduled reductions in physician payments in 2015, and providing 0.5 percent rate increases to the Medicare Part B single conversion factor through 2019. MACRA also laid the groundwork for a new quality incentive payment program called the Quality Payment Program (QPP). The QPP, launched in 2017, provides two tracks in which eligible clinicians can participate:

- Merit-based Incentive Payment System (MIPS)
- Advanced Alternative Payment Models (APMs)

Merit-based Incentive Payment System (MIPS)

MIPS is a combination of three former quality initiative programs — the Physician Quality Reporting System (PQRS), Medicare Electronic Health Record Incentive Program, or Meaningful Use, and Value-Based Payment Modifier (VM) — and one new component, which provides a single quality reporting system with a single payment adjustment factor based on individual or group performance in Medicare Part B. MIPS is a budget neutral program, meaning successful reporters earn positive payment adjustments funded by unsuccessful reporters who receive negative payment adjustments.

Per MACRA, minimum/maximum payment adjustments increase each year during the transition period:

> MIPS eligible clinicians/groups' Medicare Part B payment adjustments are based on performance thresholds. As shown in the table below, the performance threshold and payment adjustment statutorily increase each year until the maximums are reached in performance year 2021 (payment year 2023).

Payment Thresholds

Performance Period	Performance Threshold	Exceptional Performance Bonus	Payment Adjustment
2017	3 points	70 points	up to +4%
2018	15 points	70 points	up to +5%
2019	30 points	75 points	up to +7%
2020 (proposed)	45 points	80 points	up to +9%
2021 (proposed)	60 points	85 points	up to +9%

Actual payment adjustments depend on individual/group performance and the number of successful reporters in a performance period.

MIPS Eligible Clinicians

Not all Medicare Part B-enrolled providers are eligible to participate in MIPS. The definition of a "MIPS eligible clinician" is up to the discretion of CMS, and subject to change. For the initial performance years (2017-2018), MIPS eligible clinicians included:

- Physicians:
  - Doctors of chiropractic
  - Doctors of dental medicine
  - Doctors of dental surgery
  - Doctors of medicine
  - Doctors of optometry
  - Doctors of osteopathy
  - Doctors of podiatric medicine
- Nurse practitioners
- Physician assistants
- Clinical nurse specialists
- Nurse anesthetists

For the 2019 performance year, CMS redefined "MIPS eligible clinicians" to also include:

- Clinical psychologists
- Physical therapists
- Occupational therapists
- Qualified speech-language pathologists
- Qualified audiologists
- Registered dietitians or nutritionists

These MIPS eligible clinicians are automatically excluded from reporting requirements and payment adjustments if:

- They are in their first year of Medicare;
- They are Qualifying APM Participants (defined later); or
- They do not meet or exceed the "low-volume threshold."

The low-volume threshold is also subject to change per CMS discretion. The low-volume threshold finalized for the 2019 performance excludes MIPS eligible clinicians/groups who (during the determination period):

1. Have less than or equal to $90,000 in Part B allowed charges for covered professional services; or
2. Provide care to less than or equal to 200 Part B-enrolled patients; or
3. Provide less than or equal to 200 covered professional services under the Medicare Physician Fee Schedule (MPFS).

Beginning in 2019 (Year 3), MIPS eligible clinicians or groups can opt in to the program if they meet or exceed at least one (but not all three) of these criteria. Those who opt in are held to the same reporting requirements and payment adjustments as everyone else in the program.

As an alternative to opting in, clinicians who are not eligible to participate in MIPS (ie, they do not meet or exceed all three criteria) may voluntarily report quality data to CMS. Although volunteers do not qualify for +/- payment adjustments, they do receive a performance feedback report from CMS. Clinicians/groups can use this report to assess their performance and prepare for future participation in either MIPS or an Advanced APM.

Submitter Types

MIPS eligible clinicians — now referred to as *submitter types* — may submit data on measures and activities to CMS:

- Individually
- As a group
- As a virtual group
- In a MIPS APM entity

Submission Types

Submitter types submit data on measures and activities using CMS-approved submission mechanisms — now referred to as *submission types*.

There are several ways individual and group reporters can submit MIPS data to CMS, including direct, log in and upload, log in and attest, Medicare Part B claims, and the CMS Web Interface. Certain restrictions apply. For example, beginning with the 2019 performance year, only small practices (15 or fewer clinicians) may submit quality data via Medicare Part B claims, and only groups of 25 or more clinicians may submit data via the CMS Web Interface.

The MIPS performance year (when data is collected) is January 1 through December 31. Participating providers must submit their data to CMS between January 1 and March 31 following the performance year using the appropriate submission type.

Collection Types

Collection types are quality measure sets with comparable specifications and data completeness criteria such as electronic clinical quality measures (eCQMs), MIPS clinical quality measures (CQMs), qualified clinical data registry (QCDR)

measures, Medicare Part B claims measures, CMS Web Interface measures, the Consumer Assessment of Healthcare Providers & Systems (CAHPS) for MIPS survey measure, and administrative claims measures.

Beginning with performance year 2019, collector types may use a combination of collection types to submit their data (some restrictions apply).

Collection types are delineated by the four MIPS performance categories:

- Quality
- Promoting Interoperability
- Improvement Activities
- Cost

Quality

The goal of the Quality performance category is to assess the value of care to ensure patients get the right care at the right time.

MIPS eligible clinicians, groups, or virtual groups must submit at least six quality measures for the 12-month performance period. Each measure is worth a maximum of 10 points, for a maximum of 60 achievement points.

Note: The way in which measures are scored is rather complicated and beyond the scope of this training. To learn more about MIPS scoring, consider taking AAPC's MACRA Training.

The complete list of quality measures is available at https://qpp.cms.gov/mips/ quality-measures . In selecting measures on which to report, it is important to read each measure's specifications in full. These documents contain essential information.

CDEOs: Quality measure specifications relay documentation requirements for maximum achievement points. Download the 2019 Clinical Quality Measure Specifications and Supporting Documents in the Resource Library at qpp.cms.gov and locate the measures being reported by your clinicians. Use the specifications for each measure as a guide for clinical documentation improvement.

Promoting Interoperability (PI)

The goal of the Promoting Interoperability (formerly Advancing Care Information) performance category is to promote the secure exchange of health information and the use of certified electronic health record technology (CEHRT) for coordination of care.

The way in which the PI performance category is calculated changed beginning in 2019. As with the other performance categories, each measure is now scored based on the MIPS eligible clinician's performance for that measure, based on the submission of a numerator or denominator, or a yes or no submission, where applicable. The scores for each of the individual measures are added together to calculate a score of up to 100 possible points.

The four objectives and measures are:

- ePrescribing
- Health Information Exchange
- Provider to Patient Exchange
- Public Health and Clinical Data Exchange

All measures in this category can be reviewed at https://qpp.cms.gov/mips/ promoting-interoperability.

Clinicians are required to report measures from each of the four objectives for 90 continuous days, unless an exclusion is claimed from this category. In addition to submitting measures, clinicians must:

- Submit a "yes" to the Prevention of Information Blocking Attestation;
- Submit a "yes" to the ONC Direct Review Attestation; and
- Submit a "yes" for the Security Risk Analysis measure.

Individual clinicians, groups, and virtual groups can log in and attest to their PI measure data on qpp.cms.gov. Additionally, authorized third-party intermediaries can perform a direct submission on a participant's behalf.

In 2018, providers had two options based on the provider's EHR edition:

- Option 1: Program Interoperability Program Objectives and Measures
- Option 2: Program Interoperability Program Transition Objectives and Measures

Beginning with 2019, Option 2 is no longer an option; 2015 Edition CEHRT is now required for all reporters. Clinicians/ groups can apply for a PI Hardship Exception if one of the following situations applies:

- MIPS eligible clinician in a small practice (15 or fewer eligible clinicians)
- MIPS eligible clinician using decertified EHR technology
- Insufficient internet connectivity
- Extreme and uncontrollable circumstances
- Lack of control over the availability of CEHRT

Improvement Activities

The goal of the Improvement Activities performance category is to promote practice access, population management, care coordination, beneficiary engagement, patient safety and practice assessment, participation in an APM, health equity, emergency preparedness and response, and integrated behavioral and mental health.

There are approximately 90 measured activities that are designed to promote such improvements. High-weighted activities are worth 20 points and medium-weighted activities are worth 10 points each. Clinicians/Groups that hold special status (small practices, non-patient facing, rural, and Health Professional Shortage Area) receive double points for each activity.

To earn full credit in this performance category, participants must perform for 90 continuous days a combination of improvement activities that equal 40 achievement points.

All activities in this category can be found at https://qpp.cms.gov/mips/eimprovement-activities.

Participants can log in and attest to their improvement activities on qpp.cms.gov. Additionally, third-party intermediaries can perform a direct submission on a participant's behalf.

Cost

The goal of the Cost performance category is to create efficiencies in Medicare spending. No reporting/data submission is required; CMS analyzes data from both Part A and Part B claims to calculate the overall cost of patient care.

Cost measures assess a patient's total cost of care during the year or during a hospital stay, and/or during certain episodes of care. All clinicians/groups are evaluated on the same cost measures, which include:

- Total per Capita Cost measure;
- Medicare Spending per Beneficiary; and
- Episode-based measures.

Episode-based measures are categorized into two groups:

- Procedural, and
- Acute Inpatient Medical Condition group.

Procedural group measure specifications only include items and services that are related to the episode of care for a specific clinical procedure such as elective outpatient percutaneous coronary intervention, knee arthroplasty, revascularization for lower extremity chronic critical limb ischemia, routine cataract removal with intraocular lens implantation, and screening/surveillance colonoscopy.

Acute Inpatient Medical Condition group measure specifications only include items and services that are related to a specific condition such as intracranial hemorrhage or cerebral infarction, simple pneumonia with hospitalization, and ST-elevation myocardial infarction with percutaneous coronary intervention.

Achievement points for Cost measures are determined by comparing performance to a benchmark crated using performance data from the performance period.

Cost measures can be viewed at qpp.cms.gov/mips/costs.

MIPS Final Score

As shown in the table below, each performance category carries a certain amount of weight in the MIPS final score. The weights of the Quality and Cost performance categories have changed each year because MACRA requires the Cost performance category to be 30 percent of the MIPS final score by performance year 2022, and CMS is implementing that requirement in phases.

Category	Year 1 (Final Rule CY 2017, 2019 payment year)	Year 2 (Final Rule CY 2018, 2020 payment year)	Year 3 (Final Rule CY 2019, 2021 payment year)	Year 4 (Proposed Rule CY 2020, 2022 payment year)
Quality (replaced PQRS)	60%	50%	45%	40%
Promoting Interoperability (previously Advancing Care Information, replaced Meaningful Use)	25%	25%	25%	25%
Improvement Activities	15%	15%	15%	15%
Cost (replaced Value-based Modifier)	0%	10%	15%	20%

The higher the MIPS final score, the higher the payment adjustment. If you know the total points earned for each category, you can use AAPC's MIPS Score Calculator (www.aapc.com/resources/macra-calculator.aspx) to calculate your MIPS final score. Consider taking AAPC's MACRA training to learn how to step through the process of calculating a MIPS final score.

Advanced Alternative Payment Models (APM)

An APM is a group of clinicians who have voluntarily come together in an organized way to deliver coordinated high-quality care to Medicare patients. Advanced APM entities agree to:

- Use of certified EHR technology (Must be certified under 2015 criteria);
- Base payment on quality measures comparable to MIPS; and
- Either bear more than nominal risk for financial losses or is a Medical Home Model expanded under CMS Innovation Center authority.

Advanced APMs include: Bundled Payments for Care Improvement Advanced; Comprehensive End Stage Renal Disease Care – two-sided risk; Comprehensive Primary Care Plus, and others. A complete and up-to-date list of approved models is available at: https://qpp.cms.gov/apms/overview.

MIPS eligible clinicians who are on the participation list of one or more Advanced APMs during a determination period (snapshot) are not required to report MIPS data. They may also qualify for a 5 percent incentive if they achieve threshold levels of payments or patients through an Advanced APM or the All-Payer and Other Payer option. Snapshot dates are March 31, June 30, and August 31.

As an added incentive, Qualifying Participants of Advanced APMs will receive a single conversion payment factor of 0.75 percent beginning in 2024, whereas all other clinicians will receive 0.25 percent.

To learn more about MIPS APMs and Advanced APMs, consider taking AAPC's MACRA Training, available at https://www.aapc.com/training/macra-proficiency-assessment.aspx.

Glossary

Abuse—An action that results in unnecessary costs to a federal healthcare program, either directly or indirectly

Anti-kickback—Knowingly and willfully offering or accepting rewards or remuneration for services that are billable to a federal healthcare plan.

Beneficiary—An individual that is eligible for Medicare or Medicaid benefits based on the CMS guidelines

Conditions of Participation (CoP)—Conditions that healthcare organizations must meet in order to participate with the plan or program

Covered Entity—According to HIPAA, defined as health plans, healthcare clearinghouses, and healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

Criminal Healthcare Fraud Act—Scheme to willingly defraud any healthcare benefit program

False Claims Act—Federal statute setting criminal and civil penalties for falsely billing the government, over-representing the amount of a delivered product, or under-stating an obligation to the government

Fraud—Making false statements or misrepresenting facts to obtain an undeserved benefit or payment from a federal healthcare program

Health Insurance Portability and Accountability Act of 1996 (HIPAA)—Federal law in which the primary goal is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information, and help the healthcare industry control administrative costs

Preferred Provider Organization (PPO)—Managed care organization of medical doctors, hospitals, and other healthcare providers who have agreed with an insurer or a third-party administrator to provide healthcare at reduced rates to the insurer's or administrator's clients

Protected Health Information (PHI)—Individually identifiable health information that includes many common identifiers, such as demographic data, name, address, birth date, and social security number. It also includes information that relates to an individual's past, present, or future physical or mental health or condition; the provision of healthcare to the individual; or, the past, present, or future payment for the provision of healthcare to the individual, which reasonably may be used to identify an individual

Qui Tam Action—A lawsuit brought by a private citizen against a person or company who is believed to have violated the law in the performance of a contract with the government or in violation of a government regulation, when there is a statute which provides for a penalty for such violations

Stark Law—A federal law that places limitations of certain physician referrals

Truth in Lending Act—Designed to assure that every customer who needs consumer credit is given meaningful information concerning the cost of such credit