Compliance Related Topics

Medicare Cost Reports

AIHC American Institute of Healthcare Compliance

CORPORATE COMPLIANCE
WHAT YOU SHOULD KNOW

If you are a Medicare Part A or certified institutional provider, you know that every year an accurate and timely cost report must be submitted to Medicare Administrative Contractors. Your Compliance Department should be overseeing areas which can pose a high financial or legal risk to the organization. Cost reporting falls into both categories, requiring internal auditing and monitoring of this function to ensure accuracy and timeliness is observed.

Filing an inaccurate report falls under the False Claims Act, and it is critical that healthcare organizations have *trained* staff members to acquire appropriate data required to file an accurate cost report. As healthcare organizations who have been found to be noncompliant in their cost reporting will tell you, noncompliance is extremely costly for both providers and the federal government. Take a look at some recent Office of the Inspector General (OIG) audit reports to see how large the financial impacts of noncompliance can be.

Notable Cases of Noncompliant Medicare Cost Reporting

- ***Non-Compliance with Medicare Cost Reporting Requirements***

  In 2018 the Office of Inspector General (OIG) reported that the National Institute of Transplantation (NIT), an independent histocompatibility lab, did not fully comply with Medicare's cost-reporting requirements. In the cost report in question, NIT had correctly reported only 177 of 186 cost transactions. In total, the OIG estimated that NIT had received approximately $45,940 in overpayments from Medicare. OIG concluded their audit report by recommending that NIT work with the Medicare Administrative Contractor to return potential overpayments and identify any additional similar overpayments that may be related to cost reports.

- ***Referring Medicare Cost Reports and Reconciling Outlier Payments***

  A couple of years ago, two organizations were cited by OIG as not always correctly referring their Medicare cost reports to CMS. For example, Cahaba Government Benefits Administrators had only referred 5 out of 13 cost reports with outlier payments that were qualified for reconciliation to CMS. The financial impact of this noncompliance was estimated to be over $9,700,000 in total, of which just over $601,000 was due to Medicare. Another organization, CGS Administrators, had referred 15 of 18 qualified cost reports to CMS for reconciliation, but of those 15 referred reports, they had neglected to reconcile the outlier payments for 14 reports. The financial impact of these affected reports was estimated at about $39,000,000 combined, with over $16,000,000 due to Medicare.

The OIG provided both of these organizations with a number of recommendations following their audits, including:

- Review cost reports that had not been settled and should have been referred to CMS and take appropriate action to refer them to CMS so that it might recover funds due.

- Review cost reports that had been settled but were in error, determine whether these cost reports may be reopened, and work with CMS to resolve funds that may be due to the federal government.

- Review cost reports that were referred to CMS and work with CMS to finalize these reports, reconcile funds due, and return such funds to the appropriate institution.

- Improve policies and procedures to ensure the reconciliation of all qualified outlier payments associated with cost reports.

- Review all cost reports submitted since the end of OIG's audit to make sure that qualified reports and outlier payments were referred and reconciled in accordance with federal guidelines.

- ***Non Compliance with Medicare Organ Statistic Requirements***

  In 2012, LifeCenter Northwest, a federally designated independent organ procurement organization, was reported to have not fully complied with Medicare requirements for reporting organ statistics. In the affected cost report, LifeCenter had reported incorrect organ statistics for 15 different organs. In the end, Medicare's share of organ procurement costs was overstated by about $88,000. OIG recommended that LifeCenter submit a revised cost report to correct the overstatement and work to ensure that future reports followed Medicare requirements.

One of the best ways to avoid noncompliance and ensure that your healthcare organization correctly reports costs to Medicare is by utilizing professional resources and training. Follow instructions, file accurately and file on time. Consider training and even certifying staff assisting with Cost Report Preparation to train and become a Certified Cost Report Specialist (CCRS).

What You Should Know About General Health Care Compliance

Because Compliance Officers often overlook the high-risk area of cost reporting, it is important to implement internal routine auditing and monitoring to ensure data submitted is accurate and timely. As you can see in the information reported above, the government also conducts audits. This cost report review, audit, and settlement process provides a method to detect improper payments and identify the reasons these improper payments have occurred. Once identified, the reasons for the improper payments provide insight to potential payment vulnerabilities that can be used to strengthen and focus the program integrity response.

The False Claims Act or "FCA"

The False Claims Act establishes civil liability for offenses related to certain acts, including knowingly presenting a false or fraudulent claim to the government for payment, and making a false record or statement that is material to the false or fraudulent claim. Filing a false Cost Report falls under the False Claims Act.

"Knowingly" includes not only actual knowledge but also *deliberate ignorance* or *reckless disregard* for the truth or falsity of the information.

No specific intent to defraud the government is required. Individuals and entities that make false claims are subject to civil penalties of up to $11,000 for each false claim, plus three times the amount of damages the government sustains by reason of each claim.

Violation of the False Claims Act may lead to exclusion from Federal health care programs.

When you or your staff identify an overpayment within 6 years of the date the overpayment was received, generally referred to as the "look back period," you must report and return the overpayment to Medicare as outlined in Section 1128J(d) of the Social Security Act (the Act) (as added by Section 6402 of the Affordable Care Act). You must return the overpayment by the later of

1) the date 60 days after having identified the overpayment or
2) the date any corresponding cost report is due, if applicable.

Failure to return overpayments may lead to liability under the False Claims Act. Under section 1128J(d) of the Social Security Act, persons who have received an overpayment from a Federal health care program must report and return the overpayment within 60 days of the date the overpayment was identified. Failure to do so may make the overpayment a false claim.

False claims made knowingly may also be subject to criminal prosecution. Persons who knowingly make a false claim may be subject to criminal fines up to $250,000 and imprisonment of up to 5 years.

Medicare Fraud & Abuse: Prevention, Detection and Reporting

The following information is taken from the Medicare Learning Network Booklet MLN4649244 located by using the hyperlink below. It is highly recommended to download this PDF and reference it during your exam:

https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/MLN-Publications-Items/MLN4649244?DLPage=1&DLEntries=10&DLFilter=frau&DLSort=0&DLSortDir=descending

You play a vital role in protecting the integrity of the Medicare Program. To combat fraud and abuse, you need to know how to protect your organization from engaging in abusive practices and/or civil or criminal law violations. Anyone can commit health care fraud. Fraud schemes range from solo ventures to broad-based operations by an institution or group. Even organized crime has infiltrated the Medicare Program and masqueraded as Medicare providers and suppliers. Examples of Medicare fraud include:

- Billing Medicare for appointments the patient failed to keep
- Knowingly billing for services at a level of complexity higher than services actually provided or documented in the file
- Knowingly billing for services not furnished, supplies not provided, or both, including falsifying records to show delivery of such items
- Paying for referrals of Federal health care program beneficiaries

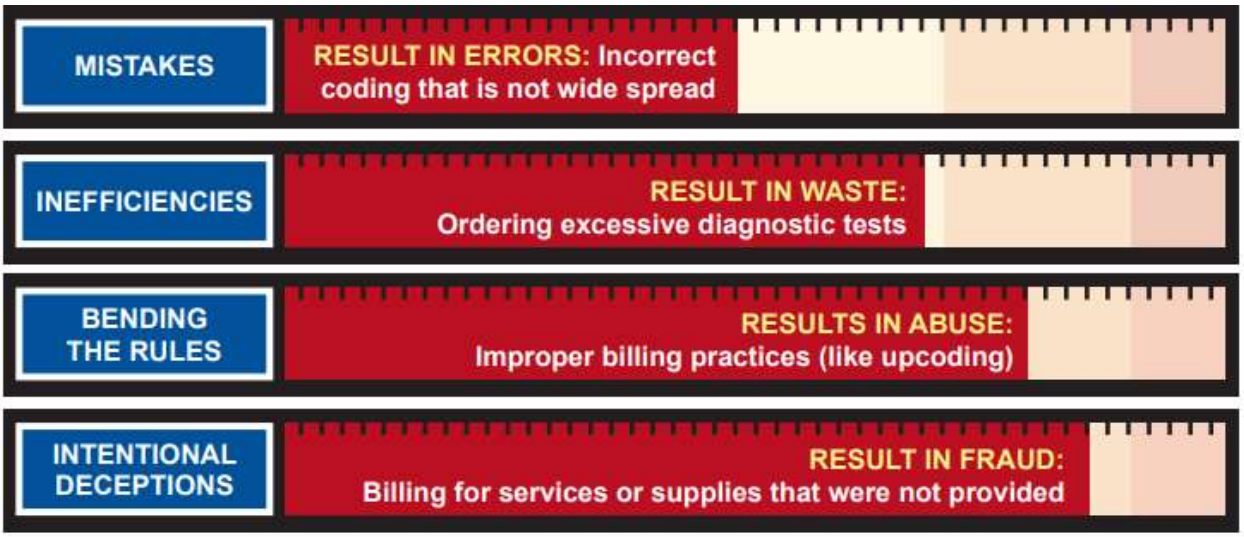
Defrauding the Federal Government and its programs is **illegal**. Committing Medicare fraud exposes individuals or entities to potential criminal and civil liability, and may lead to imprisonment, fines, and penalties. Criminal and civil penalties for Medicare fraud reflect the serious harms associated with health care fraud and the need for aggressive and appropriate intervention. Providers and health care organizations involved in health care fraud risk exclusion from participating in all Federal health care programs and risk losing their professional licenses.

Medicare Abuse

Abuse describes practices that, either directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse includes any practice inconsistent with providing patients with medically necessary services meeting professionally recognized standards. Examples of Medicare abuse include:

- Billing for unnecessary medical services;
- Charging excessively for services or supplies; and/or
- Misusing codes on a claim, such as upcoding or unbundling codes. Upcoding is when a provider assigns an inaccurate billing code to a medical procedure or treatment to increase reimbursement.

Figure 1 shows examples along the spectrum of causes of improper payments.



*The types of improper payments in Figure 1 are strictly examples for educational purposes, and the precise characterization of any type of improper payment depends on a full analysis of specific facts and circumstances. Providers who engage in incorrect coding, ordering excessive diagnostic tests, upcoding, or billing for services or supplies not provided may be subject to administrative, civil, or criminal liability.

Federal laws governing Medicare fraud and abuse include all of the following:

- False Claims Act (FCA)
- Anti-Kickback Statute (AKS)
- Physician Self-Referral Law (Stark Law)
- Social Security Act
- United States Criminal Code

These laws specify the criminal, civil, and administrative remedies the government may impose on individuals or entities that commit fraud and abuse in the Medicare Program, including Medicare Parts C and D, as well as the Medicaid Program. Violating these laws may result in nonpayment of claims, Civil Monetary Penalties (CMPs), exclusion from all Federal health care programs, and criminal and civil liability.

Additional Medicare Fraud and Abuse Penalties

Aside from the civil and criminal actions brought by law enforcement agencies, the Medicare Program has additional administrative remedies applicable for certain fraud and abuse violations.

Exclusion Statute

Excluded providers may not participate in Federal health care programs for a designated period. With very limited exception, an excluded provider may not bill Federal health care programs (including, but not limited to, Medicare, Medicaid, and State Children's Health Insurance Program [SCHIP]) for services he or she orders or performs. Additionally, an employer or a group practice may not bill for an excluded provider's services. At the end of an exclusion period, an excluded provider must seek reinstatement; reinstatement is not automatic. The OIG maintains a list of excluded parties called the ***List of Excluded Individuals/Entities*** (LEIE). Under the Exclusion Statute, the OIG must exclude providers and suppliers convicted of any of the following from participation in all Federal health care programs:

- Medicare fraud, as well as any other offenses related to the delivery of items or services under Medicare
- Patient abuse or neglect
- Felony convictions for other health care-related fraud, theft, or other financial misconduct
- Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances

Civil Monetary Penalties Law

The Civil Monetary Penalties Law authorizes CMPs for a variety of health care fraud violations. Different amounts of penalties and assessments may be authorized based on the type of violation. CMPs also may include an assessment of 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. Violations that may justify CMPs include:

- Presenting a claim, you know, or should know, is for an item or service not provided as claimed or that is false and fraudulent
- Presenting a claim, you know, or should know, is for an item or service for which Medicare will not pay
- Violating the AKS

Centers for Medicare & Medicaid Services (CMS)

CMS is the Federal agency within the U.S. Department of Health and Human Services (HHS) that administers the Medicare, Medicaid, SCHIP, Clinical Laboratory Improvement Amendments (CLIA), and several other health-related programs.

To prevent and detect fraud and abuse, CMS works with individuals, entities, and law enforcement agencies, including:

- Accreditation Organizations (AOs)
- Medicare beneficiaries and caregivers
- Physicians, suppliers, and other health care providers
- State and Federal law enforcement agencies, including the OIG, Federal Bureau of Investigation (FBI), Department of Justice (DOJ), State Medicaid Agencies, and Medicaid Fraud Control Units (MFCUs)

To support its efforts to prevent, detect, and investigate potential Medicare fraud and abuse, CMS also partners with an array of contractors, such as:

CERTs Comprehensive Error Rate Testing Contractors

MACs Medicare Administrative Contractors

MEDIC Medicare Drug Integrity Contractors

RACs Recovery Audit Program Auditors

UPICs Unified Program Integrity Contractors

ZPIC Zone Program Integrity Contractors *(Formerly called Program Safeguard Contractors or "PSC")*

Center for Program Integrity (CPI)

The Center for Program Integrity (CPI) functions within CMS and promotes the integrity of Medicare through audits, policy reviews, and identifying and monitoring program vulnerabilities. CPI oversees CMS' collaboration with key stakeholders on program integrity issues related to detecting, deterring, monitoring, and combating fraud and abuse. In 2012, CMS created the *Program Integrity Command Center* to bring together Medicare and Medicaid officials, clinicians, policy experts, CMS fraud investigators, and the law enforcement community, including the OIG and FBI. The Command Center gathers these experts to develop and improve intricate predictive analytics that identify fraud and mobilize a rapid response. CMS connects instantly with its field offices to evaluate fraud allegations through real-time investigations. Previously, finding substantiating evidence of a fraud allegation took days or weeks; now it can take only hours.

Office of Inspector General (OIG)

The OIG protects the integrity of HHS' programs, including Medicare, and the health and welfare of its beneficiaries. The OIG operates through a nationwide network of audits, investigations, inspections, and other related functions. The Inspector General is authorized to, among other things, exclude individuals and entities who engage in fraud or abuse from participation in Medicare, Medicaid, and other Federal health care programs, and to impose CMPs for certain violations related to Federal health care programs, as described above.

HIPAA: Health Insurance Portability & Accountability Act

Public Law 104-191

Medical records are some of the most personal information people have. They often reveal us at our most vulnerable. In the wrong hands, protected health information (PHI) can be used for extortion, public embarrassment or as the basis for job or other economic discrimination. Tens of millions of dollars are spent annually to make sure PHI is kept safe from prying eyes.

The Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), better known as "HIPAA", requires covered entities to apply appropriate administrative, technical, and physical safeguards to protect the privacy and security of protected health information. HIPAA Title XI Focuses on Privacy and Security related to PHI or Protected Health Information.

Reasonable care is defined as the degree of care that under the circumstances would ordinarily be exercised or expected of an average reasonable person. Physicians, hospitals, health care providers and their business associates are expected to adhere to the standards of reasonable care and are legally obligated to do so by what is known as Duty of Care. It is the primary duty of a health care professional to engage in business practices that are specific to the skill level and expertise that he or she possesses. Additionally, once a patient-physician relationship has been established, continuity of care must follow.

The law expects health care professionals to meet the average, reasonable standard of care for each similar circumstance. This standard is based on performance and is measured by what the current or prevailing circumstances are at the time of the occurrence. Therefore, a set of standards that applied two years ago, does not necessarily equate to the same standards today.

Data needed to file a Cost Report will contain protected health information of individuals, thus compliance to HIPAA privacy and security rules is something you should know. Conducting your daily duties according to your organization's HIPAA policy is an expectation for continued employment for most organizations. Breaching privacy or security standards can mean high penalties and cause a lack of trust to operate and maintain confidentiality. Additional factors come into play, such as the expectation of demonstrating consistent high ethical behavior resulting in compliance with fraud, abuse, privacy, confidentiality and security laws.

Since 1996, HIPAA law has been revised, with the most significant modifications resulting from the 2013 Omnibus Final Rule released January 25, 2013. The Omnibus Rule finalizes 4 main areas:

1. Modifications to the Privacy, Security, and Enforcement Rules to implement the Health Information Technology for Economic and Clinical Health (**HITECH**) Act, proposed in July 2010;

2. Modifications to the **Privacy Rule**, proposed in July 2010, to increase the workability of the Privacy Rule;

3. Modifies the **Breach** Notification Rule, adopted by interim final rule in August 2009; and

4. Modifications to the Privacy Rule to implement the Genetic Information Nondiscrimination Act of 2008 (**GINA**), proposed in October 2009.

The Omnibus Final Rule effective date differs from the compliance deadline. The Omnibus Rule was effective on ***March 26, 2013***. There is a provision for a compliance period of 180 days, requiring compliance as of **September 23, 2013**. The Office for Civil Rights (OCR) administers and enforces the Privacy Rule and the Security Rule.

HIPAA and Business Associates

If you are a consulting or accounting firm working with institutional providers to file Cost Reports, then you are a Business Associate.

A Business Associate is an entity that, on behalf of a covered entity but other than in the capacity of a member of the covered entity's workforce, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA. Remember, under the Final Rule, the definition of business associate now extends to subcontractors of business associates and data storage providers that maintain PHI on behalf of covered entities or business associates on a long-term basis.

A Business Associate Agreement or "BAA" is a written contract or arrangement between a covered entity and a business associate and required under HIPAA law. The BAA contract or arrangement permits the covered entity to disclose PHI to the business associate; allows the business associate to create or receive PHI on the covered entity's behalf; and allows the business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf. Every BAA must include satisfactory assurances that the business associate will appropriately safeguard PHI and/or ePHI, in accordance with the HIPAA Privacy and Security Rules.

- The BAA ***must require*** a business associate to implement the administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI; ensure that any agent or subcontractor to whom the covered entity's ePHI is provided agrees to implement appropriate safeguards; report to the covered entity any security incidents of which the business associate becomes aware; and notify the covered entity of a breach of unsecured PHI.

Business Associates and Use of Subcontractors and Agents

Covered entities should require that business associates insist that their subcontractors and agents abide by all terms of the BAA. Covered entities should also require their business associates to furnish them with a copy of any business associate subcontractors. Business associates should ensure that the BAA does not prohibit disclosure to their subcontractors and agents and does not require permission from the covered entity before making such disclosures. Business associates should also require subcontractors and agents to indemnify them to the same extent that the business associates indemnify the covered entity.

Be Mindful of HIPAA Compliance

Whether you are a Covered Entity filing the Cost Report or a Business Associate retained to assist a client to file a Cost Report, be sure your organization is compliant to applicable HIPAA rules and regulations. Seek legal counsel advice if you are in doubt, and always follow your organization's privacy and security Policies and Procedures during the Cost Report preparation and filing.

Basic HIPAA Abbreviations, Terms & Definitions

Please use the Terms and Definitions PDF to reference during your exam. Some of the HIPAA related terminology and definitions are also listed.

BAA Business Associate Agreement

- A BAA is required between health care providers and business associates.

Breach Notification Rule under HIPAA

- The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. This rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.
    - A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment

CE Covered Entity (HIPAA)

- Health care provider who conducts certain transactions in electronic form, a health plan, and a health care clearinghouse. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information – even before, during and after cost report preparation.

Confidentiality

- The property that data or information is not made available or disclosed to unauthorized persons or processes

Cybersecurity

- Broad term referring to the practice of keeping computers and electronic information safe and secure, especially during the process of e-filing your cost report and required for compliance to HIPAA law.

- According to the Office for Civil Rights (OCR – government HIPAA enforcement agency), a few cybersecurity safeguards are: Encryption, Social Engineering Awareness Training, Audit Log auditing and monitoring, Secure Configurations.

Electronic protected health information (ePHI)

- ePHI refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

Encryption

- The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and one of the cybersecurity recommendations to comply with HIPAA law.

Disposal of PHI or ePHI

- The HIPAA Privacy Rule prohibit both covered entities and business associates from simply abandoning PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.

- The HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

    - Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

HITECH

- Health Information Technology for Economic and Clinical Health Act of 2009. The HITECH Breach Notification Rule:

    - Regulations that implement provisions in the HITECH Act, part of American Recovery and Reinvestment Act of 2009 (ARRA).

    - These regulations require entities covered by HIPAA and their business associates to provide notification following a breach of unsecured PHI

Protected Health Information [PHI and ePHI] under HIPAA

- Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.

- The information relates to an individual's past, present, and future physical and mental health, the provision of healthcare to an individual, or past, present, and future payments for healthcare.

- ‘Protected’ means the information is protected under the HIPAA Privacy Rule.

    - **ePHI or Electronic Protected Health Information**
      ePHI refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

In Conclusion

Take time to understand consequences of filing a non-compliant cost report.

Be aware of potential HIPAA violations when your organization lacks appropriate Business Associate Agreements with accounting firms, legal counsel, consultants and other who may be helping your department with cost reporting or other projects.

Verify the accuracy of the data used in your cost reports. “Measure twice, cut once” is a principle which applies to cost reporting too! Measure your procedures, verify accuracy, then report once, accurately.