

Medical Staffing



- **Understanding Annual Updates to ICD 10 CM Codes**
Understanding Annual Updates to ICD 10 CM Codes Navigating CPT Code Changes for Surgical Procedures The Role of HCPCS Codes in Medical Billing Transitioning from ICD 9 to ICD 10 Challenges Specialty Specific Coding in Oncology Practices How to Avoid Errors in Evaluation and Management Coding Updates to Infectious Disease Coding Guidelines Best Practices for Using Modifiers in Medical Billing Impact of Coding Changes on Reimbursement Rates Training Resources for Mastering ICD 10 CM Coding for Chronic Conditions in Primary Care Future Trends in Medical Coding Systems
- **Key Elements of HIPAA Compliance in Medical Billing**
Key Elements of HIPAA Compliance in Medical Billing Understanding Stark Law and Its Implications Avoiding Civil Monetary Penalties in Healthcare Lessons from False Claims Act Case Studies Managing Whistleblower Risks in Medical Practices Compliance Strategies for Medicaid Billing Ethical Considerations in Medical Coding Audits Documentation Requirements for Legal Protection How to Prepare for RAC Audits Successfully State Specific Compliance Challenges in Healthcare Global Standards for Healthcare Data Privacy Training Staff on Anti Fraud Regulations
- **About Us**



In an increasingly interconnected world, the management and protection of healthcare data have become paramount. The global standards for healthcare data privacy play a crucial role in ensuring that sensitive personal information is safeguarded while still allowing the necessary flow of data to support medical advancements and patient care.

At the forefront of these standards is the General Data Protection Regulation (GDPR) enacted by the European Union. As one of the most comprehensive data protection laws, GDPR sets stringent rules on how personal data should be processed, emphasizing transparency, consent, and individuals' rights over their information. Healthcare staffing agencies provide scalable solutions for growing facilities **medical assistant staffing agency** balance sheet. Its influence extends globally as organizations outside Europe that handle EU citizens' data must also comply with its provisions.

In parallel, other regions have developed their own frameworks. The United States has the Health Insurance Portability and Accountability Act (HIPAA), which specifically addresses healthcare data privacy through regulations that protect patients' medical records and other health information provided to various entities. HIPAA mandates strict administrative, physical, and technical safeguards to ensure confidentiality and integrity.

Similarly, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private sector organizations collect, use, or disclose personal information during commercial activities. It underscores principles like accountability and limiting use to ensure personal health information is managed responsibly.

These regional standards often share core principles but can vary significantly in implementation details. As such, there are efforts to harmonize these differences through international bodies like the International Organization for Standardization (ISO). ISO/IEC 27701:2019 provides guidelines for managing privacy information management systems and serves as a bridge between various national regulations.

Despite strides in creating robust frameworks, challenges persist. The rapid pace of technological innovation outpaces legislation at times, leaving gaps in protection mechanisms. Technologies such as artificial intelligence raise new questions about consent and anonymization of data that existing laws may not fully address.

Moreover, disparities between countries' regulatory approaches can lead to complexities for multinational companies navigating cross-border data flows. There is a growing call for more universal agreements on key issues like interoperability standards to maintain both security and efficiency across borders.

In conclusion, global standards for healthcare data privacy are essential pillars supporting trust in digital healthcare ecosystems. While significant progress has been made with influential regulations like GDPR and HIPAA setting benchmarks worldwide, continuous evolution is necessary to address emerging technologies and harmonize international practices further. Only then can we ensure robust protection of individual privacy while enabling innovation in healthcare delivery globally.

In the ever-evolving landscape of healthcare, medical coding practices stand at the intersection of clinical documentation, billing, and regulatory compliance. These practices are profoundly impacted by key regulations that govern healthcare data privacy on a global scale. Understanding these regulations is crucial for ensuring that sensitive patient information is handled with the utmost care while maintaining the integrity and accuracy of medical records.

One of the most influential global standards in healthcare data privacy is the General Data Protection Regulation (GDPR) enacted by the European Union. Although it primarily applies to EU member states, its implications reach far beyond Europe due to its extraterritorial scope. The GDPR sets stringent requirements for data protection, mandating that all organizations handling personal data must implement robust security measures and obtain explicit consent from individuals before processing their information. For medical coders, this means adopting meticulous processes to ensure that any coded data used in research or shared across borders complies with GDPR's strict guidelines. This regulation emphasizes transparency and accountability, underscoring a commitment to protecting patient confidentiality while facilitating international collaboration in healthcare.

Across the Atlantic, the Health Insurance Portability and Accountability Act (HIPAA) serves as a cornerstone of healthcare data privacy in the United States. Enacted in 1996, HIPAA establishes national standards for safeguarding electronic health information through its Privacy Rule and Security Rule. Medical coding professionals must navigate these rules diligently, ensuring that any identifiable health information remains protected during coding processes. HIPAA's emphasis on confidentiality extends beyond mere compliance; it fosters trust between patients and healthcare providers by assuring them that their personal health information will not be disclosed without proper authorization.

In addition to GDPR and HIPAA, other countries have developed their own frameworks to bolster healthcare data privacy. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private sector organizations collect, use, and disclose personal information during commercial activities. Similarly, Australia's Privacy Act outlines principles for handling personal health information within its jurisdiction.

While each of these regulations has unique provisions tailored to regional needs, they share common goals: safeguarding patient privacy and enhancing data security in an increasingly digital world. For medical coders working globally or within multicountry organizations, understanding these regulatory landscapes is essential not only for compliance but also for harmonizing practices across different jurisdictions.

Moreover, global standards like those promoted by ISO (International Organization for Standardization) provide additional layers of guidance aimed at standardizing best practices in managing health data securely across borders. Adherence to such standards can facilitate smoother exchange of medical records internationally without compromising patient confidentiality-a critical aspect as telemedicine continues its rapid expansion worldwide.

In conclusion, navigating key regulations impacting medical coding practices requires vigilance towards evolving global standards for healthcare data privacy. By aligning with frameworks like GDPR and HIPAA along with country-specific laws such as PIPEDA or Australia's Privacy Act-and adhering to international guidelines-medical coders play an integral role not only in maintaining accurate clinical documentation but also upholding ethical responsibility towards protecting sensitive patient information amidst growing technological advancements in healthcare systems worldwide.

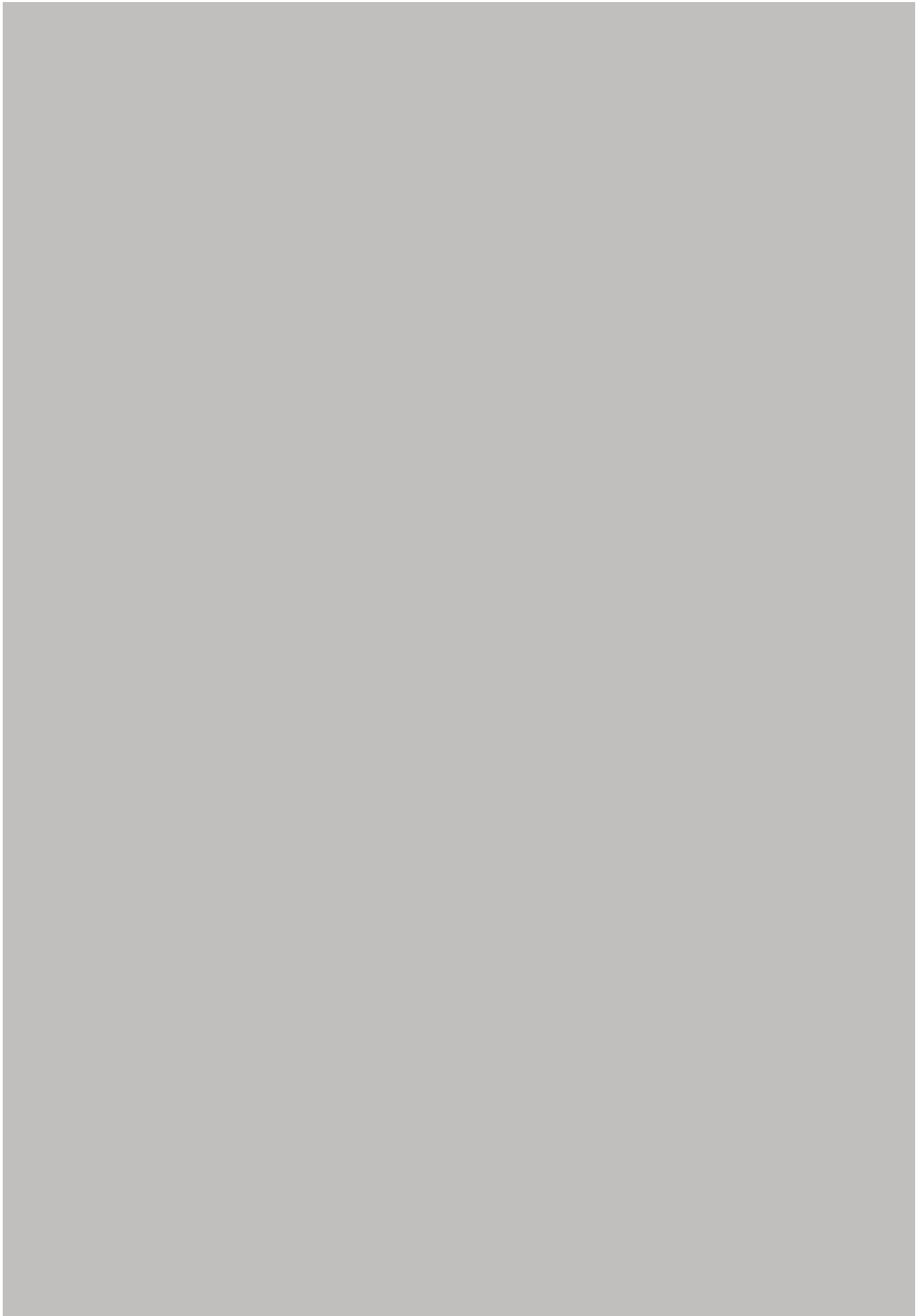
Social Sites

Instagram Channel:

"

"

More about us on X:



Key Changes and Additions to the Latest ICD-10-CM Code Set

In an increasingly interconnected world, the quest for uniform privacy standards in healthcare data has become a pressing issue. The advent of digital health technologies and the cross-border exchange of information have underscored the necessity for global standards to protect sensitive medical information. However, this endeavor is fraught with challenges that stem from diverse legal frameworks, cultural differences, technological disparities, and varying levels of resource availability.

One of the most significant hurdles in implementing uniform privacy standards globally is the wide array of legal frameworks across different countries. Each nation has developed its own set of regulations based on its unique historical, social, and political contexts. For instance, while the European Union's General Data Protection Regulation (GDPR) is often hailed as a gold standard for data protection, other regions may not have similar comprehensive legislation. Countries like the United States rely on sector-specific laws such as HIPAA (Health Insurance Portability and Accountability Act), which complicates efforts to create a cohesive global framework.

Moreover, cultural differences play a crucial role in shaping attitudes towards privacy and data sharing. In some cultures, there is an inherent trust in governmental institutions to handle personal data responsibly; in others, there is skepticism and fear regarding state surveillance or misuse of information. These cultural perceptions influence national policies and public acceptance of international standards. Achieving consensus on what constitutes appropriate data usage requires navigating these complex socio-cultural landscapes.

Technological disparities also present a formidable challenge. High-income countries are more likely to have advanced digital infrastructure capable of supporting robust privacy measures than low- and middle-income countries. This creates a gap where less technologically equipped nations struggle to implement sophisticated data protection mechanisms necessary for compliance with international standards. Bridging this technological divide necessitates substantial investment in capacity building and infrastructure development.

Additionally, resource constraints further exacerbate the difficulty of adopting uniform privacy standards globally. Many healthcare systems around the world operate under tight budgetary restrictions which limit their ability to prioritize data security initiatives over immediate clinical needs. Implementing comprehensive privacy measures requires financial resources not only for technical solutions but also for training personnel and maintaining continuous compliance monitoring.

Despite these challenges, there are promising avenues for progress toward global healthcare data privacy standards. International organizations such as the World Health Organization (WHO) can play pivotal roles by facilitating dialogue among nations and providing technical assistance to those lagging behind in technology or regulatory capacity. Collaborative efforts between governments, private sector stakeholders, non-governmental organizations (NGOs), and civil society are essential in developing flexible yet effective frameworks that respect both global imperatives and local nuances.

In conclusion, while establishing uniform privacy standards for healthcare data on a global scale is fraught with obstacles stemming from disparate legal systems, cultural perspectives on privacy rights vary widely across borders; technological gaps persist leading some countries unable even if they want too due lack resources needed achieve full implementation without help outside sources like WHO who could coordinate effort bring together different entities work collectively addressing issues head-on rather than isolationist approaches seen past attempts fall short success anticipated beforehand due difficulties encountered along way making it clear need rethink strategies moving forward ensure better future patients everywhere regardless location live within planet Earth itself given interconnected nature modern society demands nothing less than best possible outcome everyone involved process ensuring safe secure handling sensitive information entrusted care providers worldwide today tomorrow beyond all else matters most ultimately shared humanity common goal protecting preserving dignity every individual deserves right expect receive hand those charged safeguarding well-being utmost importance holds true now ever before time come act decisively collaboratively make dream reality finally once all benefit generations come reap rewards foresight determination shown present moment history written new





Impact of Updates on Healthcare Providers and Coders

In the modern landscape of healthcare, technology plays an indispensable role in advancing various facets of medical services, including data privacy in medical coding. As healthcare systems worldwide strive to protect sensitive patient information, global standards for healthcare data privacy have emerged as a critical focus area. With the growing utilization of electronic health records (EHRs) and other digital tools, safeguarding patient confidentiality has become increasingly complex and essential. This essay explores how technology enhances data privacy in medical coding while adhering to global standards.

Medical coding is a vital process that involves translating patient information into standardized codes used for billing, insurance claims, and maintaining health records. The integrity and confidentiality of this data are paramount to maintaining trust between patients and healthcare providers. As such, leveraging advanced technologies to enhance data privacy has become crucial.

Firstly, encryption technologies have been at the forefront of protecting medical data. By converting sensitive information into coded language that can only be deciphered with a specific key or password, encryption ensures that even if data is intercepted by unauthorized parties, it remains unreadable and secure. This technological approach aligns with global privacy standards like the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandate strict measures for protecting personal health information.

Moreover, blockchain technology offers promising solutions for enhancing data privacy in medical coding. Blockchain's decentralized nature ensures that once data is recorded on a block within the chain, it cannot be altered without altering all subsequent blocks—a task virtually impossible without consensus from the network majority. This immutable record-keeping makes blockchain an ideal candidate for securely storing medical codes and ensuring their accuracy over time.

Additionally, artificial intelligence (AI) and machine learning are being harnessed to detect anomalies and potential breaches more effectively than traditional methods. These technologies can monitor vast amounts of data in real-time to identify unusual patterns indicative of security threats or unauthorized access attempts. By preemptively identifying risks, AI-driven solutions enable swift responses to potential breaches before they compromise sensitive patient information.

Adherence to global standards is also facilitated by interoperability frameworks supported by technology. Interoperability ensures seamless communication between different healthcare

systems while maintaining stringent security protocols across borders. Standards such as HL7 FHIR (Fast Healthcare Interoperability Resources) provide guidelines that ensure consistent handling of patient data globally while respecting local regulations.

Despite these advancements, challenges persist-particularly concerning balancing innovation with ethical considerations around consent and user autonomy over personal health records. Healthcare organizations must remain vigilant about implementing robust cybersecurity measures alongside technological innovations without compromising individual rights or public trust.

In conclusion, technology plays an instrumental role in enhancing data privacy within medical coding underpinned by adherence to global standards for healthcare confidentiality protection practices worldwide today-and tomorrow too! Encryptions safeguard against unauthorized access; blockchain provides transparency through immutability; AI empowers proactive threat detection-all contributing towards building safer environments where patients feel confident sharing their most intimate details knowing they'll remain protected every step along their care journey ahead!

Strategies for Staying Informed About Code Changes

In the contemporary era of digital information exchange, healthcare data privacy has emerged as a critical concern worldwide. As healthcare systems become increasingly interconnected and reliant on technology, the implementation of global standards for data privacy is imperative to protect sensitive patient information. Various case studies highlight successful implementations of these standards, offering valuable insights into how countries and organizations can effectively safeguard healthcare data.

One exemplary case is that of the European Union's General Data Protection Regulation (GDPR), which has set a benchmark for data privacy across industries, including healthcare. Since its enforcement in 2018, GDPR has compelled healthcare providers within the EU to

adhere to stringent data protection measures. A notable success story under GDPR is that of a large hospital network in Germany that streamlined its data management processes to ensure compliance. By investing in robust encryption technologies and comprehensive staff training programs, the network not only enhanced its data security but also improved patient trust and engagement.

Another significant example comes from Australia with the implementation of their My Health Record system. This digital health record system was designed with privacy at its core, following global best practices and standards to protect patient information. Initially met with skepticism due to privacy concerns, extensive consultations with stakeholders led to strengthened security protocols and opt-out options for patients wary of digital records. The result was a secure platform that empowered patients while maintaining rigorous compliance with international privacy standards.

In Asia, Singapore's Integrated Health Information Systems (IHiS) offers another compelling case study. IHiS adopted a multi-layered approach to secure electronic health records by implementing advanced cybersecurity measures such as biometric authentication and regular audits for vulnerabilities. Their proactive stance on adopting international standards like ISO/IEC 27001 facilitated not only compliance but also increased resilience against cyber threats.

The United States also provides lessons through its Health Insurance Portability and Accountability Act (HIPAA). While HIPAA primarily serves national interests, it aligns closely with global standards by emphasizing patient consent and control over personal health information. Several leading American hospitals have gone beyond mere compliance by integrating advanced analytics tools governed by HIPAA guidelines to predict potential breaches before they occur.

These case studies underscore several key elements crucial for the successful implementation of global standards in healthcare data privacy: robust technological infrastructure, continuous education and training programs for staff, active stakeholder engagement, and proactive policy formulation. Moreover, they highlight that while regulations provide a necessary framework for protecting patient information, innovation in security practices plays an equally vital role.

By learning from these successes, other nations can forge pathways towards effective healthcare data privacy policies that respect cultural contexts while adhering to global norms. As we move deeper into the digital age, it becomes increasingly clear that safeguarding healthcare data through universal standards is not just about regulatory compliance; it is about building trust in an interconnected world where patient rights are paramount.



Challenges and Solutions in Adapting to New Codes

In the rapidly evolving landscape of healthcare, one of the most critical issues that has emerged is the need for robust data privacy regulations. As healthcare systems across the globe integrate more technology into their operations, safeguarding patient data becomes increasingly complex and vital. The future trends and developments in healthcare data privacy regulations are therefore pivotal in ensuring that sensitive information remains protected while facilitating innovation in medical care.

The global standards for healthcare data privacy are currently a mosaic of regional regulations, each with its unique set of rules and enforcement mechanisms. However, there is a growing consensus on the necessity for harmonization to address cross-border concerns effectively. This harmonization would not only streamline compliance for multinational organizations but also enhance collaboration among countries when dealing with pandemics or research initiatives requiring shared data.

One notable trend is an increasing emphasis on comprehensive regulatory frameworks that prioritize both security and patient consent. For instance, regions like Europe have taken significant strides with the General Data Protection Regulation (GDPR), which serves as a benchmark for other countries looking to upgrade their privacy laws. GDPR's influence can be seen in new legislation across continents aiming to provide individuals greater control over their personal health information while imposing stringent penalties for breaches.

In addition to legal frameworks, technological advancements will play a crucial role in shaping future developments in healthcare data privacy. Technologies such as blockchain and artificial intelligence offer promising solutions to enhance data security and integrity. Blockchain's decentralized nature could help reduce unauthorized access and improve transparency, while AI can automate threat detection and manage large volumes of data efficiently.

Furthermore, there is an emerging focus on ethical considerations surrounding health data usage. As technology enables more personalized medicine through genetic information and predictive analytics, questions about how this data should be used ethically without compromising individual rights are at the forefront. Regulatory bodies worldwide are thus exploring guidelines that balance innovation with ethical responsibility.

As we look ahead, international cooperation will be essential in establishing universal principles that protect patient privacy while fostering technological advancement in healthcare. Organizations like the World Health Organization (WHO) may play an instrumental role in facilitating dialogue between nations to create aligned standards that respect cultural differences yet uphold fundamental values of privacy and security.

In conclusion, as healthcare continues to digitize globally, developing coherent global standards for healthcare data privacy is imperative. Future trends point towards a convergence of stronger regulatory frameworks enhanced by cutting-edge technologies and guided by ethical considerations. By prioritizing these aspects, stakeholders can ensure that patient trust is maintained while paving the way for innovative breakthroughs in medical science.

About financial accounting



This article **needs additional citations for verification**. Please help **improve this article** by **adding citations to reliable sources**. Unsourced material may be challenged and removed.

Find sources: "Financial accounting" – news · newspapers · books · scholar · JSTOR (October 2007) (Learn how and when to remove this message)

- **v**
- **t**
- **e**

Part of **a series** on

Accounting

Early 19th-century German ledger

Image not found or type unknown

- **Constant purchasing power**
- **Historical cost**
- **Management**
- **Tax**

Major types

- **Audit**
- **Budget**
- **Cost**
- **Forensic**
- **Financial**
- **Fund**
- **Governmental**
- **Management**
- **Social**
- **Tax**

Key concepts

- **Accounting period**
- **Accrual**
- **Constant purchasing power**
- **Economic entity**
- **Fair value**
- **Going concern**
- **Historical cost**
- **Matching principle**
- **Materiality**
- **Revenue recognition**
- **Unit of account**

Selected accounts

- **Assets**
- **Cash**
- **Cost of goods sold**
- **Depreciation / Amortization (business)**
- **Equity**
- **Expenses**
- **Goodwill**
- **Liabilities**
- **Profit**
- **Revenue**

Accounting standards

- **Generally-accepted principles**
- **Generally-accepted auditing standards**
- **Convergence**
- **International Financial Reporting Standards**
- **International Standards on Auditing**
- **Management Accounting Principles**

Financial statements

- **Annual report**
- **Balance sheet**
- **Cash-flow**
- **Equity**
- **Income**
- **Management discussion**
- **Notes to the financial statements**

Bookkeeping

- Bank reconciliation
- Debits and credits
- Double-entry system
- FIFO and LIFO
- Journal
- Ledger / General ledger
- Trial balance

Auditing

- Financial
- Internal
- Firms
- Report
- Sarbanes–Oxley Act

People and organizations

- Accountants
- Accounting organizations
- Luca Pacioli

Development

- History
- Research
- Positive accounting
- Sarbanes–Oxley Act

Misconduct

- Creative
- Earnings management
- Error account
- Hollywood
- Off-balance-sheet
- Two sets of books

Financial accounting is a branch of **accounting** concerned with the summary, analysis and reporting of financial transactions related to a business.^[1] This involves the preparation of **financial statements** available for public use. **Stockholders, suppliers, banks, employees, government agencies, business owners,** and other **stakeholders** are examples of people interested in receiving such information for decision making purposes.

Financial accountancy is governed by both local and international accounting standards. **Generally Accepted Accounting Principles** (GAAP) is the standard framework of guidelines for financial accounting used in any given jurisdiction. It includes the standards, conventions and rules that accountants follow in recording and summarizing

and in the preparation of financial statements.

On the other hand, **International Financial Reporting Standards** (IFRS) is a set of accounting standards stating how particular types of transactions and other events should be reported in financial statements. IFRS are issued by the **International Accounting Standards Board** (IASB).[2] With IFRS becoming more widespread on the international scene, *consistency* in financial reporting has become more prevalent between global organizations.

While financial accounting is used to prepare accounting information for people outside the organization or not involved in the day-to-day running of the company, **managerial accounting** provides accounting information to help managers make decisions to manage the business.

Objectives

[edit]

Financial accounting and financial reporting are often used as synonyms.

1. According to International Financial Reporting Standards: the objective of financial reporting is:

To provide financial information that is useful to existing and potential investors, lenders and other creditors in making decisions about providing resources to the reporting entity.[3]

2. According to the European Accounting Association:

Capital maintenance is a competing objective of financial reporting.[4]

Financial accounting is the preparation of financial statements that can be consumed by the public and the relevant stakeholders. Financial information would be useful to users if such qualitative characteristics are present. When producing financial statements, the following must comply: **Fundamental Qualitative Characteristics:**

- **Relevance:** Relevance is the capacity of the financial information to influence the decision of its users. The ingredients of relevance are the predictive value and confirmatory value. Materiality is a sub-quality of relevance. Information is considered material if its omission or misstatement could influence the economic decisions of users taken on the basis of the financial statements.
- **Faithful Representation:** Faithful representation means that the actual effects of the transactions shall be properly accounted for and reported in the financial

statements. The words and numbers must match what really happened in the transaction. The ingredients of faithful representation are completeness, neutrality and free from error. It signifies that the accountants have acted in **good faith** during the process of representation.

Enhancing Qualitative Characteristics:

- **Verifiability:** Verifiability implies consensus between the different knowledgeable and independent users of financial information. Such information must be supported by sufficient evidence to follow the principle of objectivity.
- **Comparability:** Comparability is the uniform application of accounting methods across entities in the same industry. The principle of consistency is under comparability. Consistency is the uniform application of accounting across points in time within an entity.
- **Understandability:** Understandability means that accounting reports should be expressed as clearly as possible and should be understood by those to whom the information is relevant.
- **Timeliness:** Timeliness implies that financial information must be presented to the users before a decision is to be made.

Three components of financial statements

[edit]

Statement of cash flows (cash flow statement)

[edit]

The statement of cash flows considers the inputs and outputs in concrete cash within a stated period. The general template of a cash flow statement is as follows: *Cash Inflow - Cash Outflow + Opening Balance = Closing Balance*

Example 1: in the beginning of September, Ellen started out with \$5 in her bank account. During that same month, Ellen borrowed \$20 from Tom. At the end of the month, Ellen bought a pair of shoes for \$7. Ellen's cash flow statement for the month of September looks like this:

- Cash inflow: \$20
- Cash outflow: \$7
- Opening balance: \$5
- **Closing balance: \$20 – \$7 + \$5 = \$18**

Example 2: in the beginning of June, WikiTables, a company that buys and resells tables, sold 2 tables. They'd originally bought the tables for \$25 each, and sold them at a price of

\$50 per table. The first table was paid out in cash however the second one was bought in credit terms. WikiTables' cash flow statement for the month of June looks like this:

- Cash inflow: \$50 - *How much WikiTables received in cash for the first table. They didn't receive cash for the second table (sold in credit terms).*
- Cash outflow: \$50 - *How much they'd originally bought the 2 tables for.*
- Opening balance: \$0
- **Closing balance: $\$50 - 2 * \$25 + \$0 = \$50 - 50 = \$0$** - *Indeed, the cash flow for the month of June for WikiTables amounts to \$0 and not \$50.*

Important: the cash flow statement only considers the exchange of **actual** cash, and ignores what the person in question owes or is owed.

Statement of financial performance (income statement, profit & loss (p&l) statement, or statement of operations)

[[edit](#)]

The statement of profit or income statement represents the changes in value of a company's **accounts** over a set period (most commonly one **fiscal year**), and may compare the changes to changes in the same accounts over the previous period. All changes are summarized on the "bottom line" as **net income**, often reported as "net loss" when income is less than zero.

The net profit or loss is determined by:

Sales (revenue)

– **cost of goods sold**

– selling, general, administrative expenses (SGA)

– **depreciation**/ amortization

= earnings before interest and taxes (**EBIT**)

– interest and tax expenses

= profit/loss

Statement of financial position (balance sheet)

[edit]

The balance sheet is the financial statement showing a firm's **assets**, **liabilities** and **equity** (capital) at a set point in time, usually the end of the fiscal year reported on the accompanying income statement. The total assets always equal the total combined liabilities and equity. This statement best demonstrates the basic accounting equation:

$$\text{Assets} = \text{Liabilities} + \text{Equity}$$

The statement can be used to help show the financial position of a company because liability accounts are external claims on the firm's assets while equity accounts are internal claims on the firm's assets.

Accounting standards often set out a general format that companies are expected to follow when presenting their balance sheets. **International Financial Reporting Standards** (IFRS) normally require that companies report **current** assets and liabilities separately from non-current amounts.^{[5][6]} A GAAP-compliant balance sheet must list assets and liabilities based on decreasing liquidity, from most liquid to least liquid. As a result, current assets/liabilities are listed first followed by non-current assets/liabilities. However, an IFRS-compliant balance sheet must list assets/liabilities based on increasing liquidity, from least liquid to most liquid. As a result, non-current assets/liabilities are listed first followed by current assets/liabilities.^[7]

Current assets are the most liquid assets of a firm, which are expected to be realized within a 12-month period. Current assets include:

- **cash** - physical money
- **accounts receivable** - revenues earned but not yet collected
- Merchandise inventory - consists of goods and services a firm currently owns until it ends up getting sold
- **Investee companies** - expected to be held less than one financial period
- **prepaid expenses** - expenses paid for in advance for use during that year

Non-current assets include **fixed** or long-term assets and **intangible assets**:

- *fixed (long term) assets*
 - property
 - building

- equipment (such as factory machinery)
- *intangible assets*
 - copyrights
 - trademarks
 - patents
 - goodwill

Liabilities include:

- *current liabilities*
 - trade accounts payable
 - dividends payable
 - employee salaries payable
 - interest (e.g. on debt) payable
- *long term liabilities*
 - mortgage notes payable
 - bonds payable

Owner's equity, sometimes referred to as net assets, is represented differently depending on the type of business ownership. Business ownership can be in the form of a sole proprietorship, partnership, or a **corporation**. For a corporation, the owner's equity portion usually shows common stock, and retained earnings (earnings kept in the company). Retained earnings come from the retained earnings statement, prepared prior to the balance sheet. **[8]**

Statement of retained earnings (statement of changes in equity)

[edit]

This statement is additional to the three main statements described above. It shows how the distribution of income and transfer of dividends affects the wealth of shareholders in the company. The concept of retained earnings means profits of previous years that are accumulated till current period. Basic proforma for this statement is as follows:

Retained earnings at the beginning of period

+ Net Income for the period

- Dividends

= Retained earnings at the end of period. **[9]**

Basic concepts

[edit]

The stable measuring assumption

[edit]

One of the basic principles in accounting is "The Measuring Unit principle":

The unit of measure in accounting shall be the base money unit of the most relevant currency. This principle also assumes the unit of measure is stable; that is, changes in its general purchasing power are not considered sufficiently important to require adjustments to the basic financial statements."**[10]**

Historical Cost Accounting, i.e., financial capital maintenance in nominal monetary units, is based on the stable measuring unit assumption under which accountants simply assume that money, the monetary unit of measure, is perfectly stable in real value for the purpose of measuring (1) monetary items not inflation-indexed daily in terms of the Daily CPI and (2) constant real value non-monetary items not updated daily in terms of the Daily CPI during low and high inflation and deflation.

Units of constant purchasing power

[edit]

The stable monetary unit assumption is not applied during hyperinflation. IFRS requires entities to implement capital maintenance in units of constant purchasing power in terms of IAS 29 Financial Reporting in Hyperinflationary Economies.

Financial accountants produce financial statements based on the accounting standards in a given jurisdiction. These standards may be the **Generally Accepted Accounting Principles** of a respective country, which are typically issued by a national standard setter, or **International Financial Reporting Standards** (IFRS), which are issued by the **International Accounting Standards Board** (IASB).

Financial accounting serves the following purposes:

- producing general purpose financial statements
- producing information used by the management of a business entity for decision making, planning and performance evaluation
- producing financial statements for meeting regulatory requirements.

Objectives of financial accounting

[edit]

- **Systematic recording of transactions:** basic objective of accounting is to systematically record the financial aspects of business transactions (i.e. book-keeping). These recorded transactions are later on classified and summarized logically for the preparation of financial statements and for their analysis and interpretation.
- **Ascertainment of result of above recorded transactions:** accountant prepares profit and loss account to know the result of business operations for a particular period of time. If expenses exceed revenue then it is said that the business is running under loss. The profit and loss account helps the management and different stakeholders in taking rational decisions. For example, if business is not proved to be remunerative or profitable, the cause of such a state of affairs can be investigated by the management for taking remedial steps.
- **Ascertainment of the financial position of business:** businessman is not only interested in knowing the result of the business in terms of profits or loss for a particular period but is also anxious to know that what he owes (liability) to the outsiders and what he owns (assets) on a certain date. To know this, accountant prepares a financial position statement of assets and liabilities of the business at a particular point of time and helps in ascertaining the financial health of the business.
- **Providing information to the users for rational decision-making:** accounting as a 'language of business' communicates the financial result of an enterprise to various stakeholders by means of financial statements. Accounting aims to meet the financial information needs of the decision-makers and helps them in rational decision-making.
- **To know the solvency position:** by preparing the balance sheet, management not only reveals what is owned and owed by the enterprise, but also it gives the information regarding concern's ability to meet its liabilities in the short run (liquidity position) and also in the long-run (solvency position) as and when they fall due.

Graphic definition

[edit]

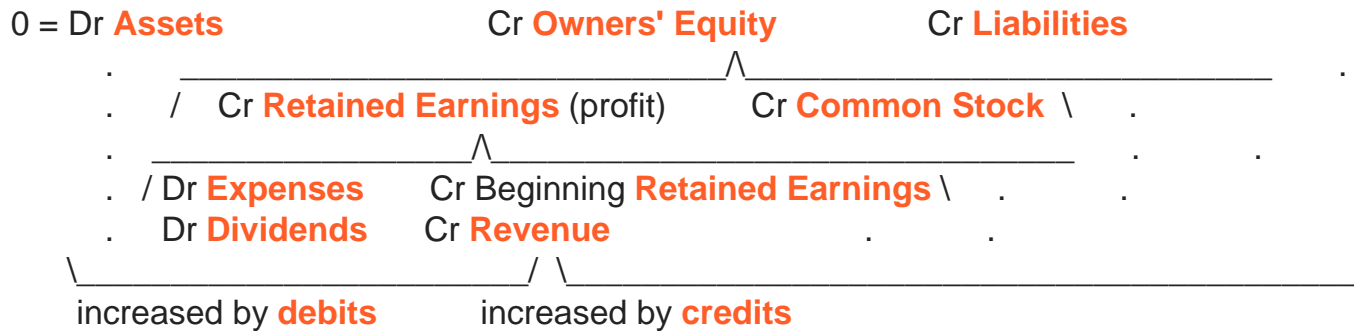
The **accounting equation** (**Assets = Liabilities + Owners' Equity**) and financial statements are the main topics of financial accounting.

The **trial balance**, which is usually prepared using the **double-entry accounting system**, forms the basis for preparing the financial statements. All the figures in the trial balance are rearranged to prepare a **profit & loss statement** and **balance sheet**. Accounting standards determine the format for these accounts (**SSAP**, **FRS**, **IFRS**). Financial statements display the income and expenditure for the company and a summary of the assets, liabilities, and shareholders' or owners' equity of the company on the date to

which the accounts were prepared.

Asset, **expense**, and **dividend** accounts have normal debit balances (i.e., debiting these types of accounts increases them).

Liability, **revenue**, and **equity** accounts have normal credit balances (i.e., crediting these types of accounts increases them).



Crediting a credit

Thus -----> account increases its absolute value (balance)

Debiting a debit

Debiting a credit

Thus -----> account decreases its absolute value (balance)

Crediting a debit

When the same thing is done to an account as its normal balance it increases; when the opposite is done, it will decrease. Much like signs in math: two positive numbers are added and two negative numbers are also added. It is only when there is one positive and one negative (opposites) that you will subtract.

However, there are instances of accounts, known as contra-accounts, which have a normal balance opposite that listed above. Examples include:

- Contra-asset accounts (such as **accumulated depreciation** and allowances for bad debt or obsolete inventory)
- Contra-revenue accounts (such as sales allowances)
- Contra-equity accounts (such as **treasury stock**)

Financial accounting versus cost accounting

[edit]

See also: **Cost accounting**

1. Financial accounting aims at finding out results of accounting year in the form of Profit and Loss Account and Balance Sheet. Cost Accounting aims at computing cost of production/service in a scientific manner and facilitate cost control and cost reduction.
2. Financial accounting reports the results and position of business to government, creditors, investors, and external parties.
3. Cost Accounting is an internal reporting system for an organisation's own management for decision making.
4. In financial accounting, cost classification based on type of transactions, e.g. salaries, repairs, insurance, stores etc. In cost accounting, classification is basically on the basis of functions, activities, products, process and on internal planning and control and information needs of the organization.
5. Financial accounting aims at presenting 'true and fair' view of transactions, profit and loss for a period and Statement of financial position (Balance Sheet) on a given date. It aims at computing 'true and fair' view of the cost of production/services offered by the firm.**[11]**

Related qualification

[edit]

Many professional accountancy qualifications cover the field of financial accountancy, including **Certified Public Accountant CPA**, **Chartered Accountant** (CA or other national designations, **American Institute of Certified Public Accountants AICPA** and **Chartered Certified Accountant (ACCA)**).

See also

[edit]

- o **Constant item purchasing power accounting**
- o **DIRTI 5**
- o **Historical cost accounting**
- o **Philosophy of accounting**
- o **Accounting analyst**, whose job involves evaluating public company financial statements
- o **Management accounting**, the other main division of accounting
- o **Bookkeeping**

References

[edit]

1. [^] **"Financial Accounting - Definition from KWHS"**. *The Wharton School*. 28 February 2011. Retrieved 13 July 2018.
2. [^] **"Who We Are - January 2015"** (PDF). *IFRS.org*. *IFRS Foundation*. Archived from *the original* (PDF) on 1 May 2015. Retrieved 28 April 2015.
3. [^] **IFRS Conceptual Framework(2010) Par. OB2**

4. ^ **European Accounting Association, Response to Question 26, Comment Letter to the Discussion Paper regarding the Review of the Conceptual Framework, on Page 2 of comment letters, dated 2014-01-24 Archived 2014-07-29 at the Wayback Machine**
5. ^ **"IAS 1 - Presentation of Financial Statements". Deloitte Global. Retrieved May 9, 2017.**
6. ^ Larry M. Walther, Christopher J. Skousen, "Long-Term Assets", Ventus Publishing ApS, 2009
7. ^ Gavin, Matt (30 August 2019). **"GAAP VS. IFRS: WHAT ARE THE KEY DIFFERENCES AND WHICH SHOULD YOU USE?"**. Harvard Business School Online. Retrieved 2 November 2020.
8. ^ Malhotra, DK; Poteau, Ray (2016). *Financial Accounting I*. Academic Publishing. **ISBN 978-1627517300**.
9. ^ Fred., Phillips (2011). *Fundamentals of financial accounting*. Libby, Robert., Libby, Patricia A. (3rd ed.). Boston: McGraw-Hill Irwin. **ISBN 9780073527109. OCLC 457010553**.
10. ^ Paul H. Walgenbach, Norman E. Dittrich and Ernest I. Hanson, (1973), New York: Harcourt Grace Javonovich, Inc. Page 429.
11. ^ *Cost and Management Accounting. Intermediate. The Institute of Cost Accountants of India. p. 17.*

Further reading

[edit]

- o David Annand, **Introduction to Financial Accounting**, Athabasca University, **ISBN 978-0-9953266-4-4**
- o **Financial Accounting** (2015) doi:10.24926/8668.0701 ISBN 978-1-946135-10-0
- o Johnny Jackson, **Introduction to Financial Accounting**, Thomas Edison State University.
- o Alexander, D., Britton, A., Jorissen, A., "International Financial Reporting and Analysis", Second Edition, 2005, **ISBN 978-1-84480-201-2**

- o **v**
- o **t**
- o **e**

Accounting

Type

- o **Financial accounting**
- o **Cost accounting**
- o **Management accounting**
- o **Forensic accounting**
- o **Fund accounting**
- o **Governmental accounting**
- o **Social accounting**
- o **Tax accounting**

- **Income statement**
- **Balance sheet**
- **Statement of changes in equity**
- **Cash flow statement**
- **Debits and credits**
- **Revenue**
- **Cost of goods sold**
- **Operating expense**
- **Capital expenditure**
- **Depreciation**
- **Gross income**
- **Net income**

Authority control databases: **National**  **Germany**  **Japan**  **Wikidata**

Frequently Asked Questions

What are the key global standards for healthcare data privacy relevant to medical coding?

The key global standards include the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in Europe, and the International Organization for Standardizations ISO/IEC 27701 standard, which provides guidelines for managing privacy information management systems. These standards ensure that patient data used in medical coding is protected against unauthorized access and breaches.

How does HIPAA impact medical coding practices?

HIPAA mandates that all entities handling Protected Health Information (PHI), including those involved in medical coding, implement safeguards to protect patient data. This includes ensuring confidentiality through secure transmission and storage of coded health information. Coders must also be trained on privacy principles to minimize risks of accidental disclosure.

What measures should be taken to comply with GDPR when processing healthcare data for medical coding?

To comply with GDPR, organizations must obtain explicit consent from patients before processing their personal data. They should also implement data minimization by only using necessary information for coding purposes, ensure transparency about how data is used, and provide mechanisms for patients to access or request deletion of their data.

Are there international efforts to harmonize healthcare data privacy standards affecting medical coding?

Yes, there are ongoing international efforts led by organizations like WHO and ISO to harmonize healthcare data privacy standards globally. These efforts aim to create a consistent framework that facilitates cross-border healthcare delivery while protecting patient privacy across different jurisdictions.

What role do coders play in maintaining compliance with global healthcare data privacy standards?

Coders play a crucial role by adhering to established protocols that safeguard patient information throughout the coding process. They must ensure accurate and secure entry of codes without disclosing identifiable patient details unnecessarily. Continuous education on

evolving privacy laws is also essential for maintaining compliance.

Altrust Services

Phone : (813) 592-3807

City : Clearwater

State : FL

Zip : 33765

Address : 3000 Gulf to Bay Blvd Suite 313

Company Website : <https://altrustservices.com/>

USEFUL LINKS

[medical staffing](#)

[medical staffing agencies](#)

[american medical staffing](#)

[consolidated medical staffing](#)

[Sitemap](#)

[Privacy Policy](#)

[About Us](#)

Follow us