Fundamentals of Law for Health Informatics and Information Management

Third Edition

Melanie S. Brodnik, PhD, MS, RHIA, FAHIMA
Laurie A. Rinehart-Thompson, JD, RHIA, CHP, FAHIMA
Rebecca B. Reynolds, EdD, MHA, RHIA, FAHIMA

AHIMA
PRESS

ISBN: 978-1-58426-530-6
AHIMA Product No.: AB241816

AHIMA Staff:

Sue Bowman, MJ, RHIA, CCS, FAHIMA, chapter contributor
Chelsea Brotherton, MA, Assistant Editor
Katherine M. Greenock, MS, Production Development Editor
Elizabeth Ranno, Vice President of Product and Planning
Pamela Woolf, Director of Publications

Cover image: ©Maxx-Studio/Shutterstock.com

Limit of Liability/Disclaimer of Warranty: This book is sold, as is, without warranty of any kind, either express or implied. While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information or instructions contained herein. It is further stated that the publisher and author are not responsible for any damage or loss to your data or your equipment that results directly or indirectly from your use of this book.

The websites listed in this book were current and valid as of the date of publication. However, webpage addresses and the information on them may change at any time. The user is encouraged to perform his or her own general web searches to locate any site addresses listed here that are no longer valid.

CPT® is a registered trademark of the American Medical Association. All other copyrights and trademarks mentioned in this book are the possession of their respective owners. AHIMA makes no claim of ownership by mentioning products that contain such marks.

For more information, including updates, about AHIMA Press publications, visit **http://www.ahima.org/education/press.**

American Health Information Management Association
233 North Michigan Avenue, 21st Floor
Chicago, Illinois 60601-5809
ahima.org

Brief Contents

Table of Contents

About the Volume Editors and Chapter Contributors

Melanie S. Brodnik, PhD, MS, RHIA, FAHIMA, is an associate professor emeritus of the undergraduate program in health information management and systems, and the graduate program in health informatics at The Ohio State University. She has served on the AHIMA Board of Directors, was president of AHIMA in 2004, and is currently serving on the board of directors of the Council on Accreditation of Health Informatics and Information Management Education (CAHIIM). She received the AHIMA Literary Award in 1992, the Champion Award in 2006, and the Legacy Award, in 2010; in 2006 she received the Ohio Health Information Management Distinguished Member Award, and received the AHIMA Distinguished Member Award and became a fellow of AHIMA in 2013. She has championed the issues of patient privacy, confidentiality, and security throughout her career. She has taught legal courses at Ohio State University and was editor and column writer for *Topics in Health Information Management* for 20 years. She served on the editorial review board for AHIMA's *In Confidence Privacy and Confidentiality Newsletter* from 1996 to 2002 and currently serves on the editorial review board of *Perspectives in Health Information Management*. She has authored or coauthored many publications and has presented at numerous local, state, and national professional association meetings, workshops, and conventions. She received her associate degree in medical record technology from Fullerton Junior College, a bachelor of science degree in health information management from Loma Linda University, a master's of science degree from the State University of New York at Buffalo, and her doctorate degree in educational research and evaluation from The Ohio State University.

Laurie A. Rinehart-Thompson, JD, RHIA, CHP, FAHIMA, is the director of the health information management and systems program and is an associate professor of clinical health and rehabilitation sciences at The Ohio State University. She earned her bachelor of science in medical record administration and her juris doctor from The Ohio State University. In addition to HIM education, her professional experiences span the behavioral health, home health, and acute care arenas. She has served as an expert witness in civil litigation, testifying as to the privacy and confidentiality of health information. She has chaired the AHIMA Professional Ethics Committee and served on numerous AHIMA committees, including the AHIMA Privacy and Security Practice Council and Council for Excellence in Education workgroups. She has served on the board of directors of the Ohio Health Information Management Association. A speaker on the HIPAA Privacy Rule, she is the author of AHIMA's *Introduction to Health Information Privacy and Security text*. She is also a contributing author to *Ethical Challenges in the Management of Health Information* and the following AHIMA publications: *Health Information Management Technology: An Applied Approach; Health Information Management: Concepts, Principles, and Practice; Documentation for Health Records; Documentation for Medical Practices; and the Journal of AHIMA*. She has been published in *Perspectives in Health Information Management*. She received the Ohio Health Information Management Association's Distinguished Member Award and the AHIMA Legacy Award in 2010, and became a fellow of AHIMA in 2011.

Rebecca B. Reynolds, EdD, MHA, RHIA, FAHIMA, is an associate professor and program director for the graduate program in health informatics and information management at the University of Tennessee Health Science Center (UTHSC) in Memphis. She has served on the AHIMA nominating committee and was chair of the 2010 AHIMA Education Strategy Committee. She is past president of the Tennessee Health Information Management Association and received its Outstanding New Professional Award in 1995 and Distinguished Member Award in 2004. She coordinated the HIPAA implementation program for the UTHSC system and provides HIPAA privacy and security training to all UTHSC students. She teaches the legal courses for both entry-level masters and post-professional graduate students and conducts legal workshops for attorneys, nurses, and other healthcare professionals. She served as a member of the Operations Committee of the Mid-South eHealth Alliance, which is a functioning health information exchange. She also serves on the Tennessee eHealth Network's Privacy and Security Work Group. She received her bachelor's degree in health information management from UTHSC and her master's degree in healthcare administration and doctorate in higher education administration from the University of Memphis. She received the AHIMA Legacy Award in 2010, and became a fellow of AHIMA in 2012.

Sue Bowman, MJ, RHIA, CCS, FAHIMA, is the senior director of coding policy and compliance for the American Health Information Management Association (AHIMA). Bowman's responsibilities include providing the association's strategic direction and leadership in the development, maintenance, adoption, and implementation of standards for terminologies, classifications, and associated data standards. She participates in a variety of AHIMA's activities pertaining to the advancement of healthcare data quality and the use of healthcare data standards. She has provided testimony to Congress and the National Committee on Vital and Health Statistics on ICD-10 and other issues pertaining to coding policy and the use of coded data.

Bowman participates in the development and maintenance of the ICD-10-CM, ICD-10-PCS, and CPT code sets. Bowman serves as AHIMA's representative to the Cooperating Parties, a group that sets national coding policy and guidance for the ICD code sets, impacting data reporting standards for the entire US healthcare industry. She also contributes to the development of international coding standards through her role as secretariat for a World Health Organization group directly involved in the development of ICD-11.

Bowman received a bachelor of science degree in medical record administration from Daemen College in Amherst, NY and a master of jurisprudence in health law degree from Loyola University Chicago School of Law.

Jill Callahan Klaver, JD, RHIA, recently retired from a long career of quality management and risk management consulting. She was principal of Health Risk Advantage, a Colorado-based risk management consulting firm that assists healthcare organizations in minimizing their risk of liability. Prior to this, she was senior vice president of public and industry leadership for AHIMA, where she helped plan and execute the association's policy and alliance agendas. Her leadership on health information management issues spans almost 40 years, and she is a frequent speaker on risk management, privacy, and electronic health information management topics. Her publications include numerous articles, chapters, and books, including chapter author of "Legal Issues in Health Information Management" in *Health Information: Management of a Strategic Resource* (Elsevier); author of *Privacy & Confidentiality of Health Information* (Jossey-Bass and AHA Press); and technical editor of *HIPAA by Example* (AHIMA). Jill served on AHIMA's Board of Directors from 2002 through 2007 and as the elected president in 2006. She was a member of the Confidentiality, Privacy, and Security Workgroup of the American Health Information Community (AHIC) of the US Department of Health and Human Services' Office of the National Coordinator for

Health Information Technology. She has a law degree from Loyola University of Chicago, a master's in administration (health administration concentration) from Central Michigan University, and a bachelor of science degree in medical record administration from Ferris State University.

Keith Olenik, MA, RHIA, CHP, is principal of The Olenik Consulting Group, LLC in Chicago, IL. He has over 30 years of experience working with healthcare delivery systems as a member of senior management and as a consultant. Olenik holds a bachelor of arts in health information management from the University of Kansas and an master of arts in health services management with an emphasis in computer resources management from Webster University. He is a member of AHIMA, currently serving on the Council for Excellence in Education, and previously served on the board of directors for AHIMA and the AHIMA Foundation.

In addition to these activities, he has been a speaker at various conventions and educational seminars on ICD-10, HIPAA, project management, legal health records, and electronic health record strategies.

Kim Theodos, JD, MS, RHIA, is currently an assistant professor of health studies at the University of Louisiana Monroe. She teaches classes related to health informatics, healthcare leadership, and healthcare administration in both on campus and online learning environments. She also serves as the program practicum coordinator and advisor for undergraduate health studies students. Previously, Kim taught as an associate professor of health informatics and information management at Louisiana Tech University. Kim's educational background includes a bachelor's degree in health information administration from Louisiana Tech University, a master's degree in healthcare management from University of New Orleans, and a juris doctor from Taft Law School.

Kim has volunteered in various capacities through the Louisiana Health Information Management Association, previously serving a term as president and currently serving as treasurer and secretary. She was recognized by LHIMA as distinguished member and outstanding volunteer. She also served on the AHIMA National Convention Planning Committee, serving as chair.

Acknowledgments

The editors would like to express appreciation to the many individuals who contributed to the writing, reviewing, and publication of this textbook. We are grateful for everyone's contributions and would particularly like to thank the AHIMA publications staff and book reviewers. We offer special recognition and gratitude to our chapter authors and coauthors Sue Bowman, Jill Callahan Klaver, and Keith Olenik, and first and second edition chapter authors and coauthors Elizabeth Bowman (chapter 16), Sebastian Proels (chapter 6), and Marcia Sharp (chapter 15).Without the collective contributions and expertise of these individuals, the publication of this textbook would not have been possible. We would also like to thank those who contributed to the first edition of the book, Joseph Brunetto, Denise Burke, Frances W. Lee, Julie Roth, and Dianne Wilkinson. Special thanks go to Mary McCain, professor emeritus, University of Tennessee, Memphis, who served as one of the editors and coauthor for the book's first edition. Her dedication and hard work on the book's first edition is greatly appreciated. Finally, the editors wish to thank their families for their support and patience during the revision process of the book.

AHIMA Press would also like to thank Judy A. Ferraro, RHIA, and Heather L. Merkley, RHIA, for their technical reviews of this text.

Online Resources

For Students

The AHIMA Press *Fundamentals of Law for Health Informatics and Information Management*, Third Edition student website includes a student workbook and a Check Your Understanding (CYU) answer key. Visit **http://www.ahimapress.org/Brodnik5306/** and scratch off the student sticker to reveal your unique student code to access the book website. Your password cannot be shared or transferred. Access to the website is for individuals only and will be terminated on publication of the next edition of this book.

For Instructors

AHIMA provides supplementary materials for educators who use this book in their classes. Materials include discussion questions and application exercises with taxonomy levels, test bank questions for each chapter with answers, PowerPoint slides, and a Check Your Understanding (CYU) answer key. Visit **http://www.ahimapress.org/Brodnik5306/** and click the link to download the PowerPoint files. Please do not enter the scratch-off code from the interior front cover, as this will invalidate your access to the instructor materials. If you have any questions regarding the instructor materials, contact AHIMA Customer Relations at (800) 335-5535 or submit a customer support request at https://my.ahima.org/messages.

Chapter 1

Introduction to the Fundamentals of Law for Health Informatics and Information Management

Melanie S. Brodnik, PhD, RHIA, FAHIMA

Learning Objectives

- Differentiate between the concepts of law, and the privacy, confidentiality, and security of health information
- Discuss why protecting the privacy and confidentiality of health information is a challenge for health information management and informatics professionals
- Discuss the difference between a paper health record, a hybrid record, and an electronic health record
- Discuss the concepts of ownership and control of the health record, how these concepts relate to the concepts of health record custodianship and stewardship, and the roles and responsibilities of the custodian or steward of health records

Key Terms

- American Recovery and Reinvestment Act of 2009 (ARRA)
- American Society for Testing and Materials (ASTM)
- Business record
- Confidentiality
- Custodian
- Custodianship
- Data security
- Electronic health record
- Electronic medical record
- Enterprise information management
- Health information exchange
- Health information technology
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health record
- Hybrid health record
- Information governance
- The Joint Commission
- Law
- Legal health record
- National Alliance for Health Information Technology
- Office of the National Coordinator for Health Information Technology
- Ownership
- Patient portal
- Personal health record
- Privileged communication
- Privacy
- Protected health information (PHI)
- Security
- Steward
- Stewardship
- System security

The complexities of managing data and information are expanding as the US healthcare industry faces increasing demands to share patient information and reduce healthcare costs while enhancing the quality and safety of patient care. There has been unparalleled interest in decreasing costs and improving the quality and safety of patient care by using **health information technology (HIT)**. The federal government has incentivized healthcare providers to move from paper to **electronic health records (EHRs)** and to share patient information through **health information exchanges (HIEs)**. The ability to integrate and share data and information from multiple sources could possibly save more than $300 billion per year in US healthcare costs (McKinsey & Company 2013). To achieve savings, individuals with access to health data and information have a legal responsibility to protect its access, use, and disclosure.

Over the last two decades, public and private efforts have been devoted to the legitimate sharing of information among multiple parties and across multiple boundaries in support of the industry's transition from fee-for-service to value-based healthcare delivery (Kloss 2015). Public and private collaborations have worked toward eliminating legal and economic barriers that prevent the compiling, storing, and sharing of electronic health information securely. Efforts have focused on identifying solutions and strategies that protect the privacy, confidentiality and security of electronically stored and exchanged health information. For example, the National Governors Association has published a roadmap to help states address barriers that prevent information flow between healthcare providers in a given state (Johnson et al. 2016). In addition, the federal Office of the National Coordinator for Health Information Technology (ONC) offers numerous guides and tools in support of nationwide sharing of health information, patient engagement, and contract negotiation between healthcare providers and EHR vendors (Henry et al. 2016; ONC 2016a; ONC 2016b).

Individuals responsible for protecting the privacy and security of health information within a healthcare organization are health information management (HIM) and health informatics professionals. They, along with healthcare administrators and providers (including physicians, nurses, dentists, and others), are challenged to understand the complexity of healthcare law and the requirements to protect the privacy, confidentiality, and security of health records and information. They must accommodate changes to laws, standards, and programmatic policies and procedures that support legal issues surrounding the delivery of healthcare and the growing use of health information and health records. It is important to have an understanding of the legal system, along with the laws, regulations, standards, and ethical considerations that arise in the delivery of safe, quality healthcare.

This chapter introduces the concept of law and the complexity of issues surrounding the growing use of HIT. It defines health information and health records and discusses the types of records commonly used in healthcare. The concepts of privacy, confidentiality, and security are discussed in terms of their significance in protecting health information. The concepts of custodial responsibility and stewardship of health records are introduced. The chapter concludes with a discussion of information and data governance as an overall means for enterprise information management.

Defining Law

Law represents a set of governing rules designed to protect citizens living in a civilized society. Law establishes order, provides parameters for conduct, and defines the rights and obligations of the government and its citizens. It controls behavior that threatens public safety and sets penalties for disobedience. There are two types of law, public and private. Public law involves federal, state, and local government and serves to define, regulate, and enforce rights and duties among individuals and businesses as related to government. For example, federal or state laws that define access, use, and disclosure of patient healthcare information represent public laws. Private law is concerned with the rules and principles that define rights and duties among individuals and among private businesses. Private law addresses issues such as contracts between two entities; for example, a contract between an EHR vendor and a hospital system.

Healthcare in the United States is a trillion-dollar industry that is highly regulated by federal and state laws, institutional accrediting bodies, professional standards of practice, and codes of ethics. These laws and standards define how healthcare is delivered, financed, and reimbursed. The laws and standards protect patients and healthcare providers by requiring accountability for services rendered, and privacy, confidentiality, and security of patient and provider health records and information. Health information may be used as evidence in legal cases when conflict arises and resolution is sought through the court system.

Health Information and Health Records

Health information refers to the data generated and collected as a result of delivering care to a patient. Its primary use is for clinical care; however, secondary uses are numerous, such as public health reporting, population health management, third-party reimbursement, quality improvement, and patient safety.

Health information is collected from multiple sources and is used for a wide variety of purposes. It is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which defines protected health information (PHI) as:

> … any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual (45 CFR 160.103).

What information is documented varies depending on several factors, including state or jurisdiction of healthcare provider, accrediting or licensing body requirements, type of healthcare provider (for example, hospital, clinic, physician practice, behavioral health center), and services rendered for the episode of care.

The information generated on a patient's episode of care comprises a patient's health record or record of care. A health record may also be known as a medical record, patient record, client record, inpatient record, outpatient record, or clinic record. The American Health Information Management Association (AHIMA) states that a health record "comprises individually identifiable data, in any medium, that are collected, processed, stored, displayed, and used by healthcare professionals" (AHIMA e-HIM Work Group 2010). It documents the care provided to the patient and the patient's healthcare status.

Health records are maintained in either paper or electronic formats, or a combination of both. The term hybrid health record refers to a record that consists of both paper and electronic records and media (for example, film, video, or imaging system) and uses both manual and electronic processes (AHIMA 2010). Electronic records may be composed of information from clinical, administrative, or financial systems, along with paper documents from internal or external sources that are scanned into the record. The data in the record may be handwritten, direct voice entry captured in a word-processing system, from provider wireless mobile devices such as phones, handheld personal computers, or any combination of these (Amatayakul 2013). Electronic and paper records may differ as summarized in figure 1.1.

If the health record is completely electronic, it is called an EHR or electronic medical record (EMR). These terms are often used interchangeably but may be defined differently depending on the organization and how the record is designed or used. To help alleviate legal barriers and facilitate adoption of EHRs and HIEs, the National Alliance for Health Information Technology (NAHIT), sponsored by the ONC, developed consensus-based definitions related to key HIT terms (NAHIT 2008). NAHIT's definitions for an EHR and EMR are as follows:

- Electronic health record: "an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization"
- Electronic medical record: "an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one healthcare organization" (NAHIT 2008, 6)

The key difference in these definitions is that the EMR is considered an electronic record housed within an organization, whereas an EHR is thought to contain data or information from more than one

Figure 1.1 Six key areas where electronic records differ from paper records

1. **Volume and Duplicability:** With advances in information technology, at least 93% of information generated today is created using digital technology. Moreover, digital information is routinely and easily duplicated. Users can easily save files and disseminate them through e-mail. Most applications used to create electronic data and files have automatic backups, which help to protect against accidental loss of data.
2. **Persistence:** It is much more difficult to dispose of electronic documents than paper documents. Paper documents can be destroyed by shredding or some other form of physical destruction. However, as noted by the court in *Zubulake v. UBS Warburg LLC*, "The term 'deleted' is sticky in the context of electronic data. Deleting a file does not actually erase the data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status—thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted even if neither the computer user nor the computer itself is aware of their existence."
3. **Dynamic Changeable Content:** Electronic information can be more easily modified than paper information. For example, correcting a spelling error on a document created using a typewriter involves physically "whiting out" the misspelled word and replacing it with the correctly spelled word. The same process is much easier in an electronic word processing application, and often only involves the use of an automatic spell checker. Further, simply accessing or moving electronic data can alter that data by changing file creation and modification dates.
4. **Metadata:** Electronic documents contain "metadata," which is "information about the document or file that is recorded by the computer to assist the computer and often the user in storing and retrieving the document or file at a later date." File designations, create/edit dates, authorship, and edit history are all examples of metadata. Where such issues are relevant or in dispute, metadata can be useful in authenticating documents or establishing exactly when documents were created. An electronic document's metadata may not be relevant in every case, especially when there is no dispute as to who authored a document or when a document was modified. However, in *Williams v. Sprint/United Mgmt. Co.*, the court held that "When a party is ordered to maintain documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact."
5. **Environment-Dependence and Obsolescence:** Unlike paper documents, electronic data may not be readable once it is moved from its "environment." For example, if a file is transferred to a different computer, that computer must have the appropriate software loaded to open that file. If it does not, then the file may not open correctly or may not be readable at all. Further, with the continual advances and upgrades of information technology, many organizations routinely migrate to new or upgraded information systems. This can make it difficult to restore electronic data or files exactly as they were maintained in previous systems.
6. **Dispersion and Searchability:** Electronic documents are easily stored in multiple locations such as on computer hard drives, servers, or portable devices such as laptops, PDAs, cell phones, or jump drives. Searching electronic documents for specific pieces of information is often less cumbersome than conducting the same search on paper. For example, a "find" or "search" function in a word processing document can quickly find all occurrences of a certain word within electronic documents regardless of their size. To find all occurrences of the same word in a large paper document could take hours of manual labor.

Source: Adapted from *The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production.*

organization. For this reason, use of the term *EHR* appears to be more prevalent, although as previously mentioned, these terms are often used interchangeably.

Healthcare consumers may also maintain a **personal health record** (PHR), which is defined as "an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual" (NAHIT 2008, 6). Healthcare providers have implemented **patient portals** that allow patients to electronically access their personal health record, and schedule appointments, communicate with their provider via e-mail messaging, and perform other functions as offered by the organization. Henry et al. (2016) reports that "there has been a significant increase in the percent of hospitals that provide patients with the ability to electronically view, download, and transmit their health information" since 2013 with an increase in patient engagement functionalities in 2015.

Whether the health record is a paper record, a hybrid record, an EMR, or an EHR, it is the legal business record created in the normal course of business of an organization or healthcare provider. It is used for business, legal, and compliance purposes. For example, it serves as evidence in lawsuits or other legal actions. Information detailing the contents of a health record, including what constitutes a legal health record, is discussed in more detail in chapter 9.

Protecting Health Records and Information

Working within healthcare requires an understanding of the American legal system, and the laws and standards that govern its delivery, financing, and reimbursement methods. Managing health data, information, and records also requires a clear understanding of laws and standards that protect the collection, access, use, exchange, and disclosure of health information and records. There is a longstanding history of state-specific and federal laws governing the privacy of health records and information. However, it was not until the passage of HIPAA (45 CFR 160, 164) in 1996 that federal rules were enacted to specifically protect patient information as a result of increasing use of information technology in healthcare. HIPAA privacy rules went into effect in 2002, followed by security rules in 2003.

Subsequently in 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) (42 USC 17921), part of the American Recovery and Reinvestment Act of 2009 (ARRA), was passed to further promote the creation of a national healthcare infrastructure through adoption and meaningful use of EHR systems by healthcare providers, and the sharing of health information through HIEs.

HITECH widened the scope of privacy and security protections under HIPAA to include companies previously not affected by HIPAA. It also provided for stricter enforcement of the rule, and increased potential legal liability for noncompliance (Callahan-Dennis 2010, 6). Many of the HITECH requirements went into effect in 2010, with the remaining requirements finalized in 2013. HIPAA and HITECH are discussed in more detail in chapters 10, 11, and 12. HIPAA and HITECH are two of more than 50 federal laws and regulations addressing privacy, confidentiality, and security protections (Office of the National Coordinator for Health IT, Privacy & Security 2016).

Core to HIPAA, HITECH, and other federal and state laws related to the protection, access, use, and disclosure of health information records is an understanding of the concepts of privacy, confidentiality, and security.

Check Your Understanding 1.1

Instructions: Indicate whether the following statements are true or false (T or F).

1. An electronic personal health record contains health-related information for an individual.
2. An EHR can be managed across more than one healthcare organization.
3. HIPAA represents a private law designed to protect patient information.
4. Patient portals are used to encourage patient engagement in their care.
5. HITECH limited the scope of privacy and security protections under HIPAA.

Privacy, Confidentiality, and Security

Privacy and confidentiality have historically been key components of the patient–provider relationship. The information contained in a health record, regardless of its scope or format, can be some of the most private and sensitive information that exists about a person. In conjunction with a healthcare encounter, documentation is created to record the care that was provided, support medical decisions, and provide evidence of patient outcomes. Patients are encouraged to be truthful with their care providers regarding their mental and physical conditions, because the truth is essential to the successful delivery of appropriate healthcare. Such truths, however, can place the patient in an extremely vulnerable position when intimate clinical and behavioral secrets are revealed or discovered as patient treatment is provided, test results are reported, and future options for care are discussed. Because of this, when a patient provides information and it is documented, there is an inherent trust that it will be kept private and protected from unauthorized access (Rinehart-Thompson and Harman 2017).

The protection of individuals' health information is a central, defining obligation of healthcare providers and health information and informatics professionals. In every area of law that relates to health information, the appropriate use and disclosure of that information must be a primary consideration. Although the protection of health information is discussed extensively later in the book, its significance warrants specific discussion in this introductory chapter. An understanding of the concepts of privacy, confidentiality, and security and the differences among the three concepts is important for the management of health information from a legal perspective.

Privacy

Privacy is an important social value that, described by jurists Samuel Warren and Louis Brandeis in 1890, means the right "to be let alone" (Rinehart-Thompson and Harman 2017). It is an important aspect of an individual's freedom and legal rights to be selective about what is revealed to others (Bankert and Amdur 2006, 143). One definition, which addresses the breadth of privacy, is provided by the American Society for Testing and Materials (ASTM) E31 Health Informatics Subcommittee, which states:

> Privacy is a right of individuals to be let [*sic*] alone and to be protected against physical or psychological invasion or the misuse of their property. It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference (ASTM Committee E31 on Healthcare Informatics Subcommittee E31.17 on Privacy, Confidentiality, and Access 2010, 4).

Although the US Constitution does not expressly grant the right of privacy, it does provide safeguards against government intrusion. Further, courts have interpreted the Constitution to give privacy rights with respect to religious beliefs (using the First Amendment as the basis), unreasonable searches (using the Fourth Amendment as the basis), marriage, and child-rearing. In addition, privacy rights have been further extended through such high-profile US Supreme Court cases such as *Griswold v. Connecticut* (contraception) and *Roe v. Wade* (abortion).

Although a constitutional right of privacy related to one's own health information is nonexistent, privacy protection has been established through other means such as court decisions, accrediting body standards, individual state laws, and federal laws like HIPAA and the HITECH provisions of ARRA. For example, the predominant accrediting body and standards-setting organization in healthcare is The Joint Commission. The Joint Commission is an independent, not-for-profit organization that evaluates and accredits more than 21,000 healthcare organizations and programs in the United States, including

- Ambulatory healthcare
- Behavioral healthcare

- Critical access hospital
- Home care and hospice
- Hospital
- Laboratory services
- Nursing care center

The accreditation standards used by The Joint Commission are designed to address an organization's level of performance in specific functional areas, such as patient treatment, patient safety, and privacy and confidentiality of information. The Joint Commission defines privacy as an individual's "right to limit the disclosure of personal information" (The Joint Commission 2016, DSCT.1). Its standards require the maintenance of information privacy, confidentiality, and security and supports efforts to ensure the integrity of data, which is the assurance that the data have not been modified without authorization or corrupted, either maliciously or accidentally (The Joint Commission 2016).

Standards of professional practice are also defined by professional healthcare organizations that offer protection of privacy rights as a main component of professional codes of ethics, as discussed in more detail in chapter 2.

Confidentiality

The terms *privacy* and *confidentiality* are often used interchangeably; however, there are important distinctions between the two terms. **Confidentiality** results from sharing private thoughts with someone else in confidence. The ASTM E31 Subcommittee on Health Informatics defines confidentiality as the "status accorded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorized individuals or organizations with a need to know" (ASTM 2010, 5).

Confidentiality, as recognized by law, stems from a relationship where information is shared between two parties such as physician and patient, attorney and client, clergy and parishioner, or husband and wife. The information or communication shared in these relationships is considered "privileged." What constitutes **privileged communication** is usually delineated by state law. Such laws in the case of healthcare providers may also further define what records of communication are privileged based on the healthcare provider's scope of practice (for example, physician, nurse, psychologist, licensed clinical social worker, or psychiatric nurse practitioner).

The concept of confidentiality of patient information resulting from a patient–provider relationship can be traced back to the fourth century BC. Hippocrates, considered the father of medicine, required Greek physicians to take the Hippocratic Oath. A modern translation of the oath includes a tenet specific to protecting the confidentiality of information shared between patient and physician:

> I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know. Most especially must I tread with care in matters of life and death. If it is given me to save a life, all thanks. But it may also be within my power to take a life; this awesome responsibility must be faced with great humbleness and awareness of my own frailty. Above all, I must not play at God (MedicineNet 2011).

Confidentiality obligates healthcare providers—individuals and organizations—to protect patient information that is collected. When a patient reveals information to a physician or other provider of care, there is a presumption that this information will be considered confidential and protected as such

(Rinehart-Thompson and Harman 2017). Healthcare organizations have the dubious task of balancing individual privacy rights and the use of confidential information to perform necessary clinical or business tasks (Herzig 2010). This includes the confidentiality of all information systems and verbal communication related to financial and business records, including employee information, as well as clinical and service communication. As with privacy, The Joint Commission also offers standards in support of confidentiality. It defines confidentiality as "protection of data or information from being made available or disclosed to an unauthorized person(s) or process(es)" (The Joint Commission 2016).

Security

The concept of **security** is related to privacy and confidentiality in that it pertains to the physical and electronic protection of information that preserves these concepts. The Joint Commission definition of security reflects all administrative, physician, and technical safeguards to "prevent unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system" (The Joint Commission 2016). The ASTM E31 Health Informatics Subcommittee defines security from two perspectives, security related to data and security related to systems:

- **Data security** is the result of effective data protection measures; the sum of measures that safeguard data and computer programs from undesired occurrences and exposure to accidental or intentional access or disclosure to unauthorized persons, or a combination thereof; accidental or malicious alteration; unauthorized copying; or loss by theft or destruction by hardware failures, software deficiencies, operating mistakes; physical damage by fire, water, smoke, excessive temperature, electrical failure, or sabotage, or a combination thereof. Data security exists when data are protected from accidental or intentional disclosure to unauthorized persons and from unauthorized or accidental alteration.
- **System security** is the totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. Security protects both the system and the information contained within from unauthorized access from without and from misuse from within. Security enables the entity or system to protect the confidential information it stores from unauthorized access, disclosure, or misuse, thereby protecting the privacy of the individuals who are the subjects of the stored information (ASTM 2010, 3).

Systems security includes cybersecurity efforts to prevent the stealing of electronically stored information. There has been an increase in the number of cyberattacks on healthcare providers in the last year, which has required providers to enhance cybersecurity protection (Dodson and Patrick 2016). From a federal perspective, the US Code on Information Security defines information security as follows:

> Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide
>
> - Integrity, which means guarding against improper information modifications or destruction, and includes ensuring information non-repudiation and authenticity
> - Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and propriety information
> - Availability, which means ensuring timely and reliable access to and use of information (National Institute of Standards and Technology 2008, A-6)

Harriet Pearson, chief privacy officer of IBM, affirmed the interdependence of privacy and security by identifying security as the way to implement an individual's expectation of privacy. "You can have outstanding security, yet violate people's perception of what their privacy ought to be. But you can't have privacy without having the right security measures in place. Privacy rests on a good security foundation always" (IBM Executive Interaction Channel 2007).

The interplay between the concepts of privacy, confidentiality and security is important since they are supported through federal and state laws accrediting body standards, and the work of numerous private and public entities concerned with the privacy, and security of EHRs and HIEs (AHIMA HIMSS HIE Privacy and Security Joint Work Group 2011).

Custodian Health Records

Ownership of the physical health record, whether paper, electronic, or hybrid, has traditionally been granted to the healthcare provider who generates the record. However, state and federal laws have long upheld the right of the patient to control the information within the record (Rinehart-Thompson 2016, 60, 63–64). Understanding who owns the health record is an important issue as healthcare providers expand their use of EHRs and HIEs. Associated with ownership of health records is the legal concept of custodianship. The custodian of health records is the individual who has been designated as having responsibility for the operational functions related to the development and maintenance of records (AHIMA e-HIM Work Group 2010). This includes the care, custody, control, and proper safekeeping and disclosure of health records, whether stored in paper or electronic format for such persons or institutions that prepare and maintain records of healthcare. An official custodian is required by both federal and state rules of evidence that permit health records to be entered as business records in legal proceedings; this is discussed further in chapter 5. The official custodian is authorized to certify (that is, verify that the record or information is what it purports to be), through affidavit or testimony, the normal business practices used to create and maintain the record (AHIMA e-HIM Work Group on the Legal Health Record 2005a, b). The custodian supervises the inspection and copying or duplication of records and can be called to testify as to the authenticity of the record.

In most healthcare organizations, those who request health information obtain it from the HIM department. The director of the HIM department (or designee) is traditionally the legal custodian of health records. In organizations that have hybrid or electronic health records, the custodian may differ depending on who is responsible for and can explain the procedures for compiling and maintaining patient information and records. This individual must also be able to validate the integrity of the information requested. See chapter 15 for a more detailed discussion of the process for releasing health information upon request or by subpoena or court order.

Regardless of the record format, patient information may be evidence in legal proceedings to allege medical negligence, assert the mental competence of an individual, or for other health or treatment issues. Individuals charged with the custodial responsibility of protecting health information act as a gatekeeper for the appropriate access, use, and disclosure of information for legitimate purposes and in conjunction with federal and state laws as well as the court system for use in legal proceedings.

Stewardship and Information Governance

With the increasing use of HIT, the role of the data or information steward is emerging. Similar to the role of custodianship, stewardship goes beyond the physical record to include "responsibilities for ensuring integrity (accuracy, completeness, timeliness) and security (protection of privacy as well as from tampering, loss or destruction) within the context of electronic information and records management"

(Davidson 2010, 42). Stewardship is a component of **information governance**. It refers to "an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements" (Johns 2015, 323). When an organization engages in **enterprise information management (EIM)**, it facilitates stewardship and overall information governance by supporting the "functions used to plan, organize, and coordinate people, processes, technology, and content for managing information as a corporate asset that ensures data quality, safety, and ease of use" (Johns 2015). The role of stewardship requires leadership, responsibility, and governance to ensure the consistent application of, and compliance with policies across organization-wide distributed information systems (Dougherty and Washington 2010, 44). Whether one is identified as a custodian or steward, key to either role is understanding the legal aspects of managing enterprise-wide information while protecting the privacy, confidentiality, and security of its access, use, and disclosure.

Check Your Understanding 1.2

Instructions: Indicate whether the following statements are true or false (T or F).

1. The US Constitution expressly grants the right of privacy to individuals.
2. Confidentiality is a legal concept designed to protect the communication between two parties.
3. Security refers to the right to be left alone.
4. Ownership of a health record generated by a physician about a patient belongs to the patient.
5. A custodian of records is responsible for certifying that a record is what it purports to be.

References

AHIMA e-HIM Work Group. 2010. Practice brief: Managing the transition from paper to EHRs. Web extra. Chicago: AHIMA. http://bok.ahima.org/doc?oid=103208

AHIMA e-HIM Work Group on the Legal Health Record. 2005a. Update: Guidelines for defining the legal health record for disclosure purposes. *Journal of AHIMA*. 76(8):64A–G.

AHIMA e-HIM Work Group on the Legal Health Record. 2005b. The Legal Process and Electronic Health Records. *Journal of AHIMA* 76(9):96A–D.

AHIMA HIMSS HIE Privacy and Security Joint Work Group. 2011. The privacy and security gaps in health information exchanges. Chicago: AHIMA. http://bok.ahima.org/PdfView?oid=104470

Amatayakul, M. 2013. *Electronic Health Records: A Practical Guide for Professionals and Organizations,* 5th ed revised reprint. Chicago: AHIMA.

American Society for Testing and Materials Committee E31 on Healthcare Informatics Subcommittee E31.17 on Privacy, Confidentiality, and Access. 2010. Standard guide for confidentiality, privacy, access, and data security principles for health information including computer-based patient records. Publication no. E1869-04(2010). Philadelphia: ASTM.

Bankert, E. and R. Amdur. 2006. *Institutional Review Board: Management and Function,* 2nd ed. Sudbury, MA: Jones and Bartlett.

Callahan-Dennis, J. 2010. *Privacy: The Impact of ARRA, HITECH and Other Policy Initiatives.* Chicago: AHIMA.

Davidson, L. 2010. From custodian to steward. *Journal of AHIMA* 81(5):42–43.

Dodson, D. and R. Patrick. 2016 (December). Horizon Report. The State of Cybersecurity in Healthcare. http://www.fortifiedhealthsecurity.com/wp-content/uploads/2016/12/Fortified-Health-Security-Horizon-Report-2016.pdf.

Dougherty, M. and L. Washington. 2010. Still seeking the legal EHR. *Journal of AHIMA* 81(2):42–45.

Henry, J., Y. Pylypchuk, and V. Patel. 2016. Electronic capabilities for patient engagement among U.S. non-federal acute care hospitals: 2012-2015. *ONC Data Brief* No. 38 (September).

Herzig, T. 2010. *Information Security in Healthcare Managing Risk.* Chicago: Health Information Management and Systems Society.

IBM Executive Interaction Channel. 2007. Privacy is good for business: An interview with Chief Privacy Officer Harriet Pearson. http://www.ibm.com.

Johns, M. 2015. *Enterprise Health Information Management and Data Governance*. Chicago, IL: AHIMA.

Johnson, K., C. Kellecher, L. Block, and F. Isasi. 2016. *Getting the Right Information to the Right Healthcare Providers at the Right Time: A Road Map for States to Improve Health Information Flow between Providers.* Washington, DC: National Governors Association Center for Best Practices.

The Joint Commission. 2016. Glossary. *Comprehensive Accreditation Manual for Hospitals: The Official Handbook. CAMH* Refreshed Core, January. http://www.jointcommission.org.

Kloss, L. 2015. *Implementing Health Information Governance Lesson from the Field*. Chicago: AHIMA.

McKinsey & Company. 2013. The big data revolution in US healthcare. Center for US Health System Reform Business Technology Office. http://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.

MedicineNet. 2011. Definition of Hippocratic Oath. http://www.medterms.com/.

National Alliance for Health Information Technology. 2008 (April). Defining key health information technology terms. http://healthit.hhs.gov.

National Institute of Standards and Technology. 2008. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. NIST Special Publication 800-66 Revision I. http://csrc.nist.gov.

Office of the National Coordinator for Health Information Technology. 2016a (December). A shared nationwide interoperability roadmap: A year in review. https://www.healthit.gov/year-in-review.

Office of the National Coordinator for Health Information Technology. 2016b (September). EHR contracts untangled. Selecting wisely, negotiating terms, and understanding the fine print. Washington, DC. https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf.

Rinehart-Thompson, L., and L. Harman. 2017. Privacy and Confidentiality. In *Ethical Challenges in the Management of Health Information*, 3rd ed. Edited by Harman, L. and F. Cornelius. Sudbury, MA: Jones and Bartlett.

Rinehart-Thompson, L. 2016. Legal Issues in Health Information Management. Chapter 2 in *Health Information Management: Concepts, Principles, and Practice*, 5th ed. Edited by Oachs, P. and A. Watters. Chicago: AHIMA.

The Sedona Conference. 2007. *The Sedona Principles: Second Edition, Best Practices Recommendations & Principles for Addressing Electronic Document Production*. https://thesedonaconference.org/publication/The%20Sedona%20Principles

Cases, Statutes, and Regulations Cited

Griswold v. Connecticut, 381 US 479 (1965).

Roe v. Wade, 410 US 113 (1973).

45 CFR 160.103: Definitions, Privacy rule. 2002.

45 CFR 160, 164: Standards for privacy of individually identified health information. 2002.

45 CFR 164.524–526: Amendment of protected health information. 2007.

42 USC 17921: Health Information Technology for Economic and Clinical Health Act. 2009.

Chapter

2

Law and Ethics

Kim Theodos, JD, MS, RHIA

Learning Objectives

- Define ethics and distinguish between law and ethics
- Differentiate between ethics and morals
- Analyze ethical theories relevant to HIM practice
- Describe the role of professional codes of ethics in protecting health information
- Explain consequences of unethical behavior
- Discuss and apply the ethical decision-making process
- Examine the ethical issues surrounding bioethics

Key Terms

- Applied ethics
- Autonomy
- Beneficence
- Bioethics
- Blanchard-Peale Ethics Check
- Code of ethics
- Conflict of interest
- Deontology
- Distributive justice
- Embryonic stem cell research
- Ethical decision-making model
- Ethical principles
- Ethics
- Hospice care
- In vitro fertilization
- Justice
- Medical ethics
- Moral values
- Morals
- Nonmaleficence
- Paternalism
- Procreation
- Professional ethics
- Professionalism
- Right-based ethics
- Utilitarianism
- Virtue-based ethics

Healthcare professionals are often faced with difficult decisions that relate to various aspects of their responsibilities. Decision-making may be influenced by reasoning from a wide variety of sources, such as culture, family, religion, law, and organization. Some decisions can be made based strictly on laws or regulations, whereas other decisions require a different source of guidance or expectation. Decision makers may be presented with a situation where a law exists, but there are complicating factors that require ethical decisions to be considered. There may also be situations in which no law or regulation exists; thus, a decision must be made based on another set of criteria, or ethics. When considering professional decisions, healthcare professionals have an obligation to adhere to laws, standards of practice, and professional codes of ethics and interpretative guidelines. As new laws and regulation grow with advances in science and technology, ethical considerations in the use of such technology are also likely to evolve. It is important for healthcare professionals to understand where the law and ethics intersect when faced with decisions in support of quality patient care. This chapter will explore the relationship between law and ethics, ethical theories and principles that facilitate ethical decision making, codes of professional conduct, models of ethical decision making, and a myriad of bioethical issues that present challenges to not only patients but also healthcare professionals.

Relationship between Law and Ethics

Law and ethics are closely intertwined. As discussed in chapter 1, law refers to a set of governing rules used to protect citizens living in a civilized society. It establishes order, provides parameters for conduct, and defines the rights and obligations of the government and citizens. In contrast, ethics reflects a culmination of individual morality, expectations of reasonable human behavior, and obligations to act appropriately based on profession or philosophy. It can also be referred to as the "formal process of intentionally and critically analyzing, with clarity and consistency, the basis for one's moral judgement" (Glover 2017, 51). A person's ethics develop from their concepts of right and wrong. Ethics functions with a set of rules of conduct that stem from moral values formed through the influence of family, culture, religion, and society. Taken together, law and ethics enable the healthcare professional to offer compassionate, competent care while adhering to governing laws surrounding the delivery, financing, reimbursement, and quality of healthcare.

Applied ethics, medical ethics, professional ethics, and bioethics are all terms relating to healthcare ethics in general. Applied ethics is a practical application of moral standards or philosophical examination of moral situations or issues. Applied ethics can be general, relating to an individual's morals and how those apply to situations. Examples of applied ethics are decisions involving issues such as the death penalty, war, gender equality, and racial division. Medical ethics is a specific type of applied ethics, because it draws upon moral principles and applies those to relevant scenarios or situations in the delivery of healthcare. A common example of medical ethics can be seen during end-of-life decisions and abortion procedures. Professional ethics are designed to provide guidance about the ethical conduct of a profession. Healthcare has various applicable codes of ethics; several will be discussed later in this chapter. Bioethics addresses matters of life and death in the use of biological and medical technology.

Throughout the healthcare continuum and across all healthcare delivery models, healthcare providers are trusted with providing quality patient care that adheres to applicable state and federal laws as well as ethical principles set forth by respective professional disciplines. Health information management and informatics professionals, as protectors of patient information and gatekeepers of data, may provide legal and ethical guidance on issues related to access, availability, and integrity of healthcare data and information.

Protecting the privacy and confidentiality of patient information is a common tenet of professional codes of ethics and numerous state and federal laws. Patients have an established right to access their information and request a copy of it, request restrictions or amendments to their information, and request confidential communication regarding their care and an accounting of disclosures. Patients can exercise these rights while also controlling what happens to their information to a certain extent. Through a signed authorization for release of information, a patient can exercise their right to control their information. Honoring those rights and protecting the privacy and confidentiality of patient health information is ingrained in law, healthcare organization policy, and the code of ethics of most healthcare disciplines.

Although federal laws provide a foundation of privacy and security regulation, more detailed policy is required to truly address the legal and ethical issues that arise from advancements in technology and changing infrastructure of individual health systems or healthcare organizations. Healthcare professionals are equipped with professional codes of ethics, decision-making frameworks, and theory-based guidance, which provide groundwork to quickly and accurately assess a situation, determine viable options, and make sound decisions. Privacy and security of patient information rests solely on the shoulders of those who access it and manage it. For example, health information management and informatics professionals must understand the privacy and security rules and regulations while upholding the measures to protect patient information. Ethical considerations may emerge when determining levels and contexts of access allowed by users to patient information. Use of ethical decision-making approaches found later in this chapter may assist the health information management or informatics professional faced with such considerations. In addition, moral values play an important part in one's overall response to an ethical issue.

Ethics and Morality

As individual as humans are, so is their moral code. **Morals** concern or relate to what is right or wrong in human behavior. Much of this stems from how someone was raised or what they were taught as a young person. Some morals stem from religious affiliations, life experiences, and theology and beliefs. The totality of beliefs, experiences, and affiliations creates someone's personal morals.

Because morals stem largely from internal sources, and ethics emerge from external obligations and expectations, some experts relate an individual's morality to the extent their psychological needs have been met or are being met. Psychologist Abraham Maslow created a hierarchy of needs denoting the most basic of physiological needs of food and water in a pyramid leading up to advanced psychological decision making and awareness. His indication was that an individual cannot achieve a high level of psychological decision making if their basic needs (bottom of the pyramid) are not met (Maslow 1943). This can be linked to someone's moral and ethical decision making as well. Consider someone who was homeless or struggling to feed themselves or their family. Their need to provide basic food and shelter for themselves and their family would become a priority. Maslow's theory is based on the idea that once basic needs are met, an individual can obtain a higher level of psychological awareness and well-being.

Personally, morals guide everyday decisions and are passed on in families as children are raised with similar beliefs and moral codes. However, a professional use of morals is considered professional ethics and comes with a higher level of decision making, because professionals draw on a broader source of information. Balancing personal and professional ethics can be difficult, especially in healthcare when not all decisions are clearly right or wrong. For example, a physician may personally disagree with an individual's decision to forgo treatment or to elect to have a certain procedure; however, a person's professional ethics must guide his or her professional decisions. This personal–professional struggle can often be seen in end of life, quality of life, and procreation treatments and procedures. Several of these dilemmas and legal implications are discussed in later chapters of the book.

Consequences of Unethical Behavior

Unethical behavior comes in many forms in healthcare and has serious consequences for both employees and managers. Hourly employees may be unethical in reporting their time worked, essentially misreporting the time they worked to get paid higher wages than they earned. Falsifying a timesheet can be interpreted as stealing from the organization and should be strictly prohibited. Another unethical behavior seen in the workplace is violating company internet policies. Spending excessive company time surfing the internet instead of working is an ethical issue in many departments today. Also, employees who use the internet to visit prohibited websites, such as social media sites, would be considered unethical. The issue with these actions is related to the reduction in productivity when employees are not doing their jobs. Consequences of these behaviors could include fewer or no pay increases, poor performance reviews, and disciplinary actions such as reduction of duties or access, verbal warnings, written warnings, suspension, and termination.

Individuals in positions of authority, such as supervisors and managers, are also at risk of unethical behavior while conducting their business, because of their position and the power they possess. Nondisclosure or underreporting of incidents or breaches is an example of an unethical behavior.

A HIM or informatics professional may wish to not disclose incidents because they may fear the negative repercussions. Because they are often in the position to make decisions in the organization, healthcare vendors or companies selling items may approach them to purchase their product or service. Vendors or sales companies may offer to take the manager to lunch or offer them an item of nominal value. A manager accepting these items could appear to be taking a bribe in return for purchasing or contracting with that vendor or salesperson. HIM or informatics managers must be careful to stay in compliance with guidelines set forth by their compliance department and the AHIMA Code of Ethics, covered later in this chapter, or the state they work in if their actions are ethical. Unethical behavior may result in loss of respect; loss of credibility with peers, and loss of position in the organization.

Ethical Theories

Throughout history, philosophers and theorists have developed ethical concepts and frameworks, many of which date back hundreds of years. These ethical theories vary widely in how they are derived and applied. Some theorists take a logical approach, valuing consequences or duty over virtue. However, others hold morals and essential rights over outcome. A review of a few valid theories is important to understand how ethical standards have emerged and how they can each be applied to ethical predicaments and to the healthcare professional. The HIM and informatics professional may use one or several of these theories as they are faced with ethical dilemmas and must make difficult decisions.

Utilitarianism is an ethical theory based on the idea that the best option in an ethical decision relates to which choice provides the greatest advantage or benefits the greatest number of people. Therefore, the suitability of an ethical decision depends solely on the outcomes; fundamentally, the benefit justifies the cost or the means. This theory can apply to a healthcare organization in allocation and utilization of resources. Often, in healthcare, decisions to invest organizational funds are based on what will make the most difference financially or improve patient care. The options that result in higher reward or that effect more patients would be selected under the utilitarianism theory. However, this theory does not consider situations in which the organization is required by law to implement new initiatives that may not result in the greatest benefit. When an organization is required to comply with a law, there exists a duty to act. The outcome is not considered (Fremgen 2016).

Deontology is derived from the word duty. Another term for deontology is *duty-based ethics*. Instead of the result or outcome shaping decisions, as in utilitarianism theory, the obligation to perform your duty is the critical concept in deontology. It can be explained that the creation of duty has already weighed good versus bad, and duty exists only to do good (Allen 2013); thus individuals tend to feel it is their duty to follow the laws of their government. Duties may also arise from religious affiliations, moral obligations, or even employment relationships. One argument against the deontology theory is that duties can vary from one person to another. One person may feel an obligation to act in a certain way whereas someone else does not experience that obligation. This could lead to inconsistencies in ethical decision making (Fremgen 2016). In healthcare, a duty exists in the physician–patient relationship. Often, healthcare providers feel obligated to the patient's successful outcome, even after discharge. A physician or nurse staying after their shift ends to monitor a patient would be an example of deontology in healthcare ethics.

Right-based ethics is based on the idea that every individual has certain rights. Maintaining those rights should be the overall goal and the primary ethical consideration. Although considering every individual's rights (both legal and perceived) is an ideal approach, there may be a conflict between two individuals who both have rights. For example, an employee complains that his or her rights have been violated by a hospital policy against smoking on hospital campus. The hospital maintains a right to create policies that may restrict actions of its employees but are essential to maintain a professional and healthy environment. These two existing rights may conflict, and using rights-based ethics may not help in determining the best option (Fremgen 2016).

Virtue-based ethics can be viewed as seeking the “good life.” Dating back to the philosopher Aristotle, this theory of ethics focuses on the happiness found in our intrinsic characteristics and virtues. Without considering consequences, this approach values an individual’s positive moral principles that lead them to do positive things. The idea that healthcare professionals elect their profession because they possess the virtue to innately want to do good is an example of virtue-based ethics. Of course, there are times that this innate virtue is overcome by selfishness, greed, or malice found either in the individual or in others who may take advantage of a virtuous person (Fremgen 2016).

Each ethical theory has substantial benefits and strong reasoning and can influence ethical healthcare decisions. Where one theory has strong ethical undertones, another may have thorough justification. A combination of these theories is the best approach to guiding ethics in the healthcare organization.

Ethical Principles

A principle is a guiding foundation used to determine a course of action. To facilitate decision making as related to right or wrong, four **ethical principles** can be used to assist healthcare professionals in addressing healthcare-related dilemmas (Beauchamp and Childress 2012). Those principles are autonomy, beneficence, nonmaleficence, and justice. Although universally accepted as ethical principles, each uniquely provides healthcare professionals a foundation upon which decisions can be based. A thorough understanding of each principle is critical to defining ethical issues and establishing reasoning.

Autonomy

Autonomy is recognizing the right of a person to make one’s own decision, or self-determination. The ability to control what happens to your own body is an integral right of a human that is protected by law but also rooted in ethics. The principle of autonomy is at the forefront of the informed consent process, which will be discussed in chapter 8. A patient must demonstrate competence to maintain autonomy and the ability to make their own decisions. Competence is derived from a patient’s age, mental status, and capacity to make sensible decisions. Once a patient reaches the age of majority, they are legally able to make their own healthcare decisions unless their mental status either temporarily or permanently prevents them from making sound decisions (Beauchamp and Childress 2012).

Two challenges to a patient’s autonomy include paternalism and right-to-die decisions. **Paternalism** arises when a medical professional’s opinion on how the patient should act is considered above the patient’s opinion or personal preferences. It often threatens to supersede a patient’s autonomy. Although patients should trust their physicians and caregivers and listen to their advice and educated opinions, their ideas should not supplant the patient’s ability to make independent decisions.

Beneficence

Beneficence can be defined as doing good, promoting the health and welfare of others, demonstrating kindness, showing compassion, and helping others. Compassion and kindness are at the forefront of healthcare, with beneficence guiding the activities of providers every single day (Beauchamp and Childress 2012). One major challenge a provider may face is when a patient or their family demands more care or additional services the provider knows to be futile. Consider a terminally ill patient whose family is trying to decide whether to put that patient on a ventilator and sustain their life. An ethical conflict often is realized when families request additional services or attempts at resuscitation. The caregiver's ethical principle of beneficence is challenged, weighing the idea of promoting health and welfare and showing compassion for a patient who is dying.

Nonmaleficence

All physicians take an oath upon entering practice "to do no harm." This is called the Hippocratic Oath, and it speaks directly to the next ethical principle called **nonmaleficence**. Defined as doing no harm, this principle protects patients from care that will injure or further hurt them. Although physicians and other caregivers do not typically intend to injure patients or cause harm, it does happen. Medical malpractice and negligence lawsuits often result from unintentional harm done to patients. Chapter 6 will discuss the liability assumed when such harm occurs.

Administration of certain types of medications can have both positive and negative effects. For example, powerful chemotherapy medications have very specific benefits for cancer patients that have been well-documented and researched. However, those medications can also cause severe side effects for the patients who take them. Chemotherapy patients often experience constant fatigue, nausea and vomiting, pain, and hair loss. The benefits of the medication must outweigh the side effects for nonmaleficence to stay intact.

Justice

Justice is known as the obligation to be fair in the distribution of benefits and risks. At first glance, justice may not seem related to healthcare; however, the ethical ideas of benefits and risks, the right to care, and what is owed to patients apply to the healthcare industry. The availability of high-quality healthcare to all Americans, as well as the injustice of illness and cost of treatment are all issues surrounding the principle of justice. Some identify healthcare as a "benefit" to be distributed to those who seek care, whereas others hold the idea of healthcare as a human right. If healthcare is a benefit to be distributed, someone must determine the definition of "fairness" in relation to each patient request. In addition, risk assumed by patients' actions often leads to ethical decisions. Lifelong smokers put themselves at a greater risk for certain diseases, just as skydivers take known risks when they jump out of a plane. Should risky actions be awarded the same distribution of benefits? Or should all patients expect the same distribution of benefits regardless of cost, risk, or disregard for potential danger?

Examining the concept of justice more closely, the terms *fairness* and *impartiality* emerge as indicative of the ethical challenges faced. Allocation of scarce and costly healthcare resources is a source of much debate and varying theory. **Distributive justice** focuses on fair apportionment of resources to all patients, considering several factors including ability to pay, need, equity, and potential benefit of resources. Many theorists support use of distributive justice because it includes more determinants for decision making, and it also considers the unique aspects of providing healthcare services to patients (Neuberger and Swirsky 2017, 250).

Check Your Understanding 2.1

Instructions: Indicate whether the following statements are true or false (T or F).

1. Psychologically, an individual will seek fulfillment of their basic needs before considering ethical repercussions of their actions.
2. The level of ethics increases as responsibility and position in the industry increases.
3. When a patient refuses treatment, he or she is exercising the ethical principle of beneficence.
4. The ethical principle of nonmaleficence refers to making sure rules are fairly and consistently applied to all.

Codes of Professional Conduct

Professionalism

Professionalism can be interpreted as the conduct or qualities that characterize or mark a profession or a professional person. At the center of the idea of professionalism is the profession itself. The profession is established around a core set of competencies or technical abilities. The members of a profession regulate themselves and establish their own expectations (Kirk 2007). As in any other industry, there are certain characteristics intrinsic to the HIM profession. For example, HIM professionalism reflects the expected knowledge base of the profession, the nature of the occupations within the profession, and the licenses, credentials, or certifications that often identify members of the profession. Although ethics can certainly play a role in professionalism, there is a clear distinction between the two terms. Professionalism may change based on age, education, position, or work setting, whereas ethics remain consistent across all areas and levels of practice. The ethical behavior of an HIM director is the same as that expected of a coder. Although professionalism denotes the conduct marking a profession as a whole, ethics is much more comprehensive, encompassing professional ethics, personal ethics, and morals.

Conflicts of Interest

Professional ethics may be challenged when a professional is faced with a conflict of interest. A **conflict of interest** occurs when there is a conflict between private or personal interests and the official responsibilities of a person in a leadership position. An individual may be presented with situations in which they or someone they know could benefit personally or financially from decisions made. For example, a physician practice has decided to hire an agency to clean their office after hours. The professional's spouse owns a commercial janitorial service and offers the spouse's company name as a recommendation. This would be considered a conflict of interest because the individual or someone closely aligned with the individual stands to benefit from the individual's decision or influence on the decision. The decision appears to be self-serving and unethical, and in some cases, it may even be illegal. Healthcare professionals in decision-making positions are often required to sign a conflict of interest agreement. This statement expresses the individual's understanding of conflicts of interest and gives an opportunity to disclose any known conflicts. Many states prohibit state employees or their family members from entering into contracts that would be considered conflicts of interest (Louisiana Code of Governmental Ethics 2015). The legality of an act does not correlate with the ethical nature of that same act, so because something is not prohibited legally does not mean that is ethical or that it is not a conflict of interest. Determining the ethical nature of an act takes reasoning and weighing of benefits and risks. Conflicts of interest often pit ethics against personal satisfaction or personal or financial gain. Codes of professional conduct, ethics, and interpretative guidelines can assist professionals in navigating through these types of ethical problems. In addition, in certain situations, laws have been enacted that define issues of conflict of interest.

Code of Ethics

The ideal is to uphold laws while demonstrating the moral values and ethical principles defined by one's professional code of ethics. A **code of ethics** reflects the values and principles defined by a profession as acceptable behavior within a practice setting. It represents the guiding principles by which a profession governs the conduct of its members. Health informatics and information management professionals face unique decisions related to privacy, security, and confidentiality; collection, maintenance, and storage of patient information; and integrity and accessibility of patient information (AHIMA 2011a). Since codes of ethics represent standards of ethical practice, they are often used as a benchmark for acceptable practice in malpractice, negligence, or other litigious situations. Codes of ethics are dynamic in that they change as societal and practice expectations change. A brief overview of several prominent healthcare professional associations and their codes of ethics will be discussed, including the American Health Information Management Association (AHIMA), the American Medical Association (AMA), and the American Medical Informatics Association (AMIA).

American Health Information Management Association (AHIMA)

The ethical principle of protecting patient privacy has been a cornerstone and an inherent core value and ethical obligation within the AHIMA Code of Ethics since the beginning of the profession in 1928. The discipline of HIM focuses on the process and systems for managing health information and records required to deliver quality healthcare to the public. HIM professionals work in a variety of businesses and health-related settings, and may be found in departments throughout organizations. They may have oversight responsibility for upholding federal and state laws regarding practices related to documentation, reimbursement, quality of care, employee and overall privacy, confidentiality, and security of health information. They are cognizant of the policies, procedures, rules, and regulations that allow for the legitimate fulfillment of requests for access, use, release, or disclosure of health information.

AHIMA created its code of ethics to guide conduct and decision making of HIM professionals. The code of ethics not only assists HIM professionals in their daily mission to protect patient information and improve quality of care, it also creates an expectation of patients and coworkers about what type of conduct they can anticipate from AHIMA members. With this expectation also emerges an appreciation for the HIM professional's expertise in the protecting the privacy and security of patient health information. The AHIMA Code of Ethics is firmly rooted in establishing positive relationships between HIM professionals, healthcare organizations, and the patients they serve. Figure 2.1 depicts the 11 specific ethical focuses for AHIMA and its members. Much of the code of ethics focuses on advancing the HIM profession in a positive, honorable manner through continuing education and mentoring of new professionals. Each principle is further enhanced by interpretive guidelines that can be accessed on the AHIMA website referenced at the end of the chapter. There are several examples of how the AHIMA Code of Ethics provides guidance for examining ethical issues related to complex work situations, such as pressure to upcode, underreport delinquent records, and deny professional development (Crawford 2011).

There is a need to balance the appropriate and lawful use of health information with the protection of the patient's privacy. Although all healthcare providers must be vigilant about protecting patient privacy, the HIM professional is often the individual designated by an organization to address privacy issues; protect patient information from unauthorized, inappropriate, and unnecessary intrusion; and make day-to-day operational decisions about disclosures and release of information policies and procedures. Core to the profession's *code of ethics* are Tenets I, III, and IV, which specifically address protecting the privacy and confidentiality of health information and records. The interpretive guidelines for these principles are shown in figure 2.2.

Tenet I states that the professional must "advocate, uphold, and defend the individual's right to privacy and the doctrine of confidentiality in the use and disclosure of information" (AHIMA 2011a). As shown in figure 2.2, this tenet implies that there is an obligation to maintain confidentiality of the patient's information, honor their right to privacy through ensuring proper access and use of that information, and be an active advocate for the patient's right to privacy. HIM professionals are called to actively participate in privacy and confidentiality through workforce training, consistent monitoring of safeguards, and by effectively ensuring those accessing the patient's information have such authority.

Figure 2.1 AHIMA Code of Ethics

Preamble

The ethical obligations of the health information management (HIM) professional include the safeguarding of privacy and security of health information; disclosure of health information; development, use, and maintenance of health information systems and health information; and ensuring the accessibility and integrity of health information. Healthcare consumers are increasingly concerned about security and the potential loss of privacy and the inability to control how their personal health information is used and disclosed. Core health information issues include what information should be collected; how the information should be handled, who should have access to the information, under what conditions the information should be disclosed, how the information is retained and when it is no longer needed, and how is it disposed of in a confidential manner. All of the core health information issues are performed in compliance with state and federal regulations, and employer policies and procedures. Ethical obligations are central to the professional's responsibility, regardless of the employment site or the method of collection, storage, and security of health information. In addition, sensitive information (e.g., genetic, adoption, drug, alcohol, sexual, health, and behavioral information) requires special attention to prevent misuse. In the world of business and interactions with consumers, expertise in the protection of the information is required.

Ethical Principles: The following ethical principles are based on the core values of the American Health Information Management Association and apply to all health information management professionals.

Health information management professionals:

I. Advocate, uphold, and defend the individual's right to privacy and the doctrine of confidentiality in the use and disclosure of information.

II. Put service and the health and welfare of persons before self-interest and conduct themselves in the practice of the profession so as to bring honor to themselves, their peers, and to the health information management profession.

III. Preserve, protect, and secure personal health information in any form or medium and hold in the highest regard the contents of the records and other information of a confidential nature, taking into account the applicable statutes and regulations.

IV. Refuse to participate in or conceal unethical practices or procedures.

V. Advance health information management knowledge and practice through continuing education, research, publications, and presentations.

VI. Recruit and mentor students, peers, and colleagues to develop and strengthen professional workforce.

VII. Represent the profession accurately to the public.

VIII. Perform honorably health information management association responsibilities, either appointed or elected, and preserve the confidentiality of any privileged information made known in any official capacity.

IX. State truthfully and accurately their credentials, professional education, and experiences.

X. Facilitate interdisciplinary collaboration in situations supporting health information practice.

XI. Respect the inherent dignity and worth of every person.

Source: AHIMA 2011a.

Tenet III states that the professional must "preserve, protect, and secure personal health information in any form or medium and hold in the highest regard the contents of the records and other information of a confidential nature obtained in the official capacity, taking into account the applicable statutes and regulations"(AHIMA 2011a). The HIM professional's obligation does not end with the patient's health record. Knowing all the places where patient data is stored, transmitted, and created electronically is both a challenge and an ethical obligation according to this tenet. To safeguard patient data from unauthorized access and disclosure, that data must be secured in all formats. Again, the AHIMA Code of Ethics calls

Figure 2.2 AHIMA Code of Ethics interpretive guides for protecting health information and records

I. Advocate, uphold, and defend the individual's right to privacy and the doctrine of confidentiality in the use and disclosure of information.

Health information management professionals shall:

1.1. Safeguard all confidential patient information to include, but not limited to, personal, health, financial, genetic, and outcome information.

1.2. Engage in social and political action that supports the protection of privacy and confidentiality, and be aware of the impact of the political arena on the health information issues for the healthcare industry.

1.3. Advocate for changes in policy and legislation to ensure protection of privacy and confidentiality, compliance, and other issues that surface as advocacy issues and facilitate informed participation by the public on these issues.

1.4. Protect the confidentiality of all information obtained in the course of professional service. Disclose only information that is directly relevant or necessary to achieve the purpose of disclosure. Release information only with valid authorization from a patient or a person legally authorized to consent on behalf of a patient or as authorized by federal or state regulations. The minimum necessary standard is essential when releasing health information for disclosure activities.

1.5. Promote the obligation to respect privacy by respecting confidential information shared among colleagues, while responding to requests from the legal profession, the media, or other non-healthcare related individuals, during presentations or teaching and in situations that could cause harm to persons.

1.6. Respond promptly and appropriately to patient requests to exercise their privacy rights (e.g., access, amendments, restriction, confidential communication, etc.). Answer truthfully all patients' questions concerning their rights to review and annotate their personal biomedical data and seek to facilitate patients' legitimate right to exercise those rights.

III. Preserve, protect, and secure personal health information in any form or medium and hold in the highest regard the contents of the records and other information of a confidential nature obtained in the official capacity, taking into account the applicable statutes and regulations.

Health information management professionals shall:

3.1. Safeguard the privacy and security of patients' written and electronic records and other sensitive information. Take reasonable steps to ensure that health information is stored securely and that patients' data are not available to others who are not authorized to have access. Prevent inappropriate disclosure of individually identifiable information.

3.2. Take precautions to ensure and maintain the confidentiality of information transmitted, transferred, or disposed of in the event of a termination, incapacitation, or death of a healthcare provider to other parties through the use of any media.

3.3. Inform recipients of the limitations and risks associated with providing services via electronic media (such as computer, telephone, fax, radio, and television).

IV. Refuse to participate in or conceal unethical practices or procedures and report such practices.

Health information management professionals **shall not**:

4.6. Participate in, condone, or be associated with dishonesty, fraud and abuse, or deception. For example,

- Allowing patterns of retrospective documentation to avoid suspension or increase reimbursement
- Assigning codes without physician documentation
- Failing to report licensure status for a physician through the appropriate channels
- Recording inaccurate data for accreditation purposes
- Allowing inappropriate access to genetic, adoption, or behavioral health information
- Misusing sensitive information about a competitor
- Violating the privacy of individuals
- Coding when documentation does not justify the diagnoses or procedures that have been billed
- Coding an inappropriate level of service
- Miscoding to avoid conflict with others
- Engaging in negligent coding practices

Source: AHIMA 2011a.

the professional to take an active role in managing patient information by taking steps to identify and safeguard patient information. Notably, this obligation remains throughout the patient's continuum of care, even if the healthcare provider no longer exists.

Tenet IV takes a different approach, because it addresses what an HIM professional should *not* do. Refusal to participate in, condone, or be associated with unethical behavior ensures that the professional maintains integrity, honesty, and ethics in all duties (AHIMA 2011a). Several of the unethical behaviors listed in Tenet IV have been discussed as ethical challenges in this chapter. Using the AHIMA Code of Ethics as a guide for best practice is the optimal display of professionalism and high ethical standards for a health information management professional.

Complementing the Code of Ethics Tenets I, III, and IV is AHIMA's Consumer Health Information Bill of Rights (AHIMA 2011b). AHIMA created the bill for the purpose of educating healthcare consumers about the protections and safeguards related to their personal health information. The bill validates every individual's right to lawful access of their personal health information, expectation of protection and prevention of unauthorized access, assurance of accuracy of their record; and an expectation for appropriate remedy when these privileges are violated (AHIMA 2011b). While the document is designed for healthcare consumers, it also offers those responsible for managing health information additional knowledge for ethical decision making regarding the protection and release of health information.

American Medical Association (AMA)

Ethical principles related to privacy and confidentiality have been inherent to the practice of medicine since the fourth century BC, when the Hippocratic Oath was created and "appealed to the inner and finer instincts of the physician" (American Medical Association 2007). The AMA, from its first established code of ethics in 1847 to its most recent update in 2016, has upheld the preservation of patient confidentiality through its code of medical ethics. Principle IV of the code states, "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law." The principles are then further explained in related chapters (Brotherton et al 2016). Chapter 3 of the code of ethics offers more specific guidelines on privacy, confidentiality, and medical records. Specifically, Sections 3.3.2 and 3.3.3 address electronic storage of patient records. Section 3.3.2 provides guidance for physicians when selecting an electronic system, including user access controls for authorized individuals, data integrity, and practices for releasing and sharing information electronically. Section 3.3.3 discusses the ethical obligation of a physician to both ensure confidentiality of electronic records and report breaches of confidentiality (AMA 2016). This update and revision of the AMA code of ethics addresses major changes in the healthcare industry involving the use of information technology in patient care. As the industry changes, so do the ethical codes guiding these professionals.

American Medical Informatics Association (AMIA)

Another professional group that addresses the appropriate use and protection of health information is AMIA. This not-for-profit organization supports the transformation of healthcare through science, education, research, and practice in biomedical and health informatics (AMIA 2010). Members of AMIA are asked to uphold the organization's code of professional ethical conduct, which specifically addresses the use of patient information in its first ethical guideline (see figure 2.3). The code also offers ethical guidance as related to patients, employers, colleagues, society, research, and general performance.

As with AHIMA's Code of Ethics, the AMIA guidelines focus on directing informatics professionals in serving as an expert in their organizations while meeting the needs and honoring the rights of patients.

AMIA also specifically addresses the ethical use of electronic information and research using patient information. Another goal is to ensure the accessibility and usability of patient information for colleagues and other healthcare professionals (AMIA 2013).

The first principle found in the AMIA code of ethics closely resembles the tenets of the AHIMA code. AHIMA focuses on protecting the patient's information while protecting individual patient rights, and this is paralleled in the AMIA principle found in figure 2.3. AMIA discusses the potential harm that exists when improper disclosures occur, thereby focusing on the importance of mitigating that risk. The remaining ethical code focuses on those functions integral to the informatics profession, such as research, data governance, and technological approaches to improving quality of care (AMIA 2013).

Check Your Understanding 2.2

Instructions: Indicate whether the following statements are true or false (T or F).

1. Conflicts of interest can be unethical as well as illegal.
2. A code of ethics should guide patient behavior.
3. The HIM professional's ethical duty ends when the patient's record is complete.
4. A profession's code of ethics should be created and maintained by individuals in that profession.
5. AHIMA created the Consumer Health Information Bill of Rights for the purpose of educating healthcare providers about the protections and safeguards related to health information.

Ethical Decision Making

Ethics Committee

Healthcare organizations recognize the need for a standardized approach to ethical decision making and education of their workforce. An ethics committee is commonly found in healthcare organizations.

Figure 2.3 AMIA principles of professional ethical conduct related to protecting health information

I. Key ethical guidelines regarding patients, guardians, and their authorized representatives (called here collectively "patients"):

A. Given that patients have the right to know about the existence and use of electronic records containing their personal healthcare information, AMIA members involved in patient care should:

1. Not mislead patients about the collection, use or communication of their healthcare information;
2. Enable and-as appropriate, within reason and the scope of their position and in accord with independent ethical and legal standards, facilitate patients' rights to access, review, and correct their electronic healthcare information. Further, they should:

B. Advocate and work as appropriate to ensure that health and biomedical information is acquired, stored, analyzed and communicated in a safe, reliable, secure and confidential manner, and that such information management is consistent with applicable laws, local policies, and accepted informatics processing standards.

C. Never knowingly disclose biomedical data in violation of legal requirements or accepted local confidentiality practices, or in ways that are inconsistent with the explanation of data disclosure and use previously given to the patient. AMIA members should understand that inappropriate disclosure of biomedical information can cause harm, and so should work to prevent such disclosures. Likewise, even if an action does not involved disclosure, one should not use patient data in ways inconsistent with the state purposes, goals, or intentions of the organization responsible for these data—except as appropriate for approved research, public health or reporting as required under the law.

Source: American Medical Informatics Association 2013.

The ethics committee's function is to contemplate, analyze, and make recommendations for addressing complex ethical problems (Hurst et al. 2005) The committee must consider the mission of the organization, any religious affiliations of the organization that may impact their approach to the ethical issue or resolution of the issue, and the applicable laws or regulations. Furthermore, participants on the committee must understand all of these factors as well as the professional ethics that organizational employees may be held to (Judicial Council 1985).

In addition to an internal recognition of a need for an ethics committee, external sources have identified the value of an ethics committee as well. The Joint Commission, an accrediting body for healthcare organizations, requires accredited healthcare institutions to provide a mechanism by which the organization promotes a "culture of ethical practices and decision making." In their Governance, Leadership, and Direction standards, The Joint Commission addresses ethics from the patient rights, financial, and clinical perspectives (The Joint Commission n.d.). Even the judicial system has recognized the need for a review body within healthcare to advise providers on ethical decisions. In the first right-to-die case involving Karen Quinlan, the judges actually discussed a need for an official committee to review and assist decision making, basically denoting these issues as questions of medical ethics rather than law (*In re Quinlan*1976).

Models of Ethical Decision Making

Ethics and ethical decisions permeate every department, function, and system in healthcare today. Because all individuals have different sets of moral codes, those responsible for ethics training must standardize ethical decisions. When everyone sees right and wrong a little differently or follows different codes of ethics, it can be extremely difficult to manage the risk of someone's decisions. The privacy and security challenges found in healthcare can be approached from a legal perspective using laws such as HIPAA and HITECH as justification; however, ethical challenges should be approached using a standardized set of steps such as those described next in this section. Whereas an ethical code is a set of guidelines, a model of ethical decision making provides specific steps that can be used to approach any ethical decision. In their Ethics & Compliance Toolkit, the Ethics and Compliance Initiative (ECI) created an **Ethical Decision-Making Model** that can easily be used in healthcare ethics decision (ECI n.d.). This method of ethical decision making assumes a multistep approach.

Steps in Ethical Decision Making

1. Define the problem
2. Seek out relevant assistance, guidance, and support
3. Identify alternatives
4. Evaluate the alternatives
5. Make the decision
6. Implement the decision
7. Evaluate the decision (ECI n.d.)

The initial steps involve clarifying the ethical issue and gathering facts. Understanding the problem includes understanding whether the decision calls upon ethics, morals, laws, or other controlling regulations. Defining the ethical issue helps the decision maker clarify what specifically has to be decided. Considering the facts of the issue, as well as those individuals or stakeholders involved, is crucial to fully understanding the decision required. This process may involve making inquiries to other parties or witnesses, reviewing relevant documentation or reports, and observing behaviors or actions. Once the issue is clearly defined, applicable laws, codes of ethics, and organizational policies and procedures may help guide the decision-making process. These guidelines and best practices can assist a decision maker by providing an objective standard on which to base a decision. Applicable policies, organizational mission and vision, and affiliations must all be considered in these decisions, because they often guide decisions throughout the organization. Certain actions may be against hospital policy, and thus the best decision becomes apparent through careful review of those policies (ECI n.d.).

Once all information about the problem has been gathered, analyzed, and reviewed, all options should be considered. A decision maker must be knowledgeable of all alternatives available before determining whether they are viable options. This should be an inclusive process rather than exclusive. When evaluating options, the HIM and informatics professional must weigh expected benefits and outcomes against potential risk and challenges. This reasoning can be the most difficult aspect of the decision-making process, because many competing interests may be involved, and a complex decision may have various options or alternatives. After all alternatives are exhausted, the optimal option is determined. Once a decision is made, all focus turns to implementing that decision, educating those it will affect, and monitoring the outcome. Some decisions have subsequent effects on other individuals or situations, similar to a domino effect. Ideally, this effect would have been predicted in the evaluation step, and the individuals affected by the decision would have been prepared. However, the domino effect can be unpredictable. In this case, part of the evaluation and reflection would be centered on managing the potential negative effects or new decisions presented as a result (ECI n.d.).

Another reputable decision-making guideline is known as the **Blanchard-Peale Ethics Check** (1988). They suggest a three-prong approach to making a decision about an ethical problem. The following questions are asked:

1. Is it legal? For example, a HIM or informatics professional would examine applicable laws and regulations or company policy. In essence, if the answer to this question is “no,” that resolves the ethical problem or action. That option would not be considered if it violates a law or policy.
2. Is it balanced? If the ethical action will more heavily favor one party over the other, the decision is not balanced. The HIM or informatics professional would weigh the benefits to one party versus another party to determine fairness, a term that is quite subjective. Comparing the advantage to one party against the other is one way to determine if an action or decision is fair and balanced.
3. How will it make me feel about myself? This asks the HIM or informatics professional to reference his or her own personal feelings about the decision. If a negative emotion is experienced when considering an option, perhaps that is not the optimal choice (Blanchard and Peale 1988).

These step-by-step approaches to ethical decision making assist in breaking down complex situations into manageable and understandable steps. Ethical decisions, especially in healthcare may cause emotional conflict and uncertainty. HIM and informatics decisions can range from coding to management, with multiple factors contributing to potential outcomes. Utilizing a standardized process for decision making eliminates some of the uncertainty and emotional distress when weighing alternatives and options. When uncertainty is eliminated, an HIM or informatics professional can be confident in a decision and can support that decision with sound reasoning and justification. Ethical decision making is often not a singular activity, but one that includes input for a variety of individuals, especially in cases where human health and life are concerned. With rapid advances in science and technology, the field of bioethics has emerged.

Bioethics

The term *bioethics* first emerged in the late 1960s when rapid advancements were made in biological research involving animals. Scientists identified and anticipated the rapid change in medical technology and advancement of new treatments (Khushf 2004). Bioethics in general can be defined as ethical issues that arise as a result of advancements in healthcare disease detection, medication interventions, and enhanced treatments. Bioethical concerns range from beginning-of-life decisions, including abortion and contraception, to end-of-life decisions, including euthanasia. New technologies developed to support advancements in stem cell research and reproduction have ethical considerations and are the subject of much debate. Many bioethical issues have been addressed through the courts and in some cases through laws designed to protect the privacy and security of patient information. Advancements in technologies have "extended the power to control, explain and predict human attributes and life processes … with this power comes the ethical dilemma of 'We can do it, but should we?'" (Science Reference Services 2015). Some issues that have arisen as a result of biological and medical advances are discussed in later sections.

Ethical Dilemmas at the Beginning and End of Life

Ethical decisions relating to **procreation**, or the beginning of life, have presented themselves in determining when life begins and identifying the product of life. Many research studies have focused on the issues, risks, and expected outcomes of the science and technologies that relate to procreation. One type of procedure that is widely used is **in vitro fertilization (IVF)**, which refers to the act of fertilization outside of the woman's body. Typically, a number of the woman's eggs are fertilized with a male's sperm during IVF. The fertilized eggs are then introduced into the woman's uterus. The fertilized eggs that are not used are often frozen so that they may be used later if the procedure is not successful the first time or if the woman decides to use IVF again for a later pregnancy. Ethical issues have arisen in regard to the disposition of frozen eggs and sperm if the partners divorce or one of them dies. For example, in the case of *Davis v. Davis*, ownership and disposition of the frozen fertilized eggs after the couple decided to end their marriage arose. Mr. Davis struggled ethically with his ex-wife's wishes to donate the fertilized eggs to couples who could not conceive. The court found that the ethical concerns of Mr. Davis outweighed his ex-wife's wishes to donate the eggs, thus finding in favor of Mr. Davis's desire not to donate the eggs.

Another issue related to fertilized frozen eggs is **embryonic stem cell research**. Embryonic stem cells are harvested from unused donated fertilized embryos acquired through an IVF process. When the eggs are no longer needed, the couple may decide to donate those fertilized eggs for research purposes. Studies have shown these cells to be particularly beneficial in treating Down syndrome and Parkinson's disease as well as many degenerative diseases. The benefit of these cells versus the ethical issues surrounding their procurement has been the subject of much debate and litigation. Some argue that fertilized eggs have the potential to become human life or are even in the beginning stages of human life. Others argue that these cells have not yet become human life, and thus the benefits associated with using them for research and possibly treatment are enough to support their use.

Preventing procreation through contraception and sterilization can also involve ethics and morals. Prescription and use of contraceptives, especially by minors or in religiously affiliated institutions, is often strictly controlled or even prohibited. There are various forms of contraceptives, including pharmaceuticals, physical barriers, or other temporary implantable devices that prevent conception. A permanent form of controlling procreation is known as sterilization. Sterilization in a male patient is accomplished through a vasectomy and in a female patient through tubal ligation. Both of these procedures prevent conception by permanently altering the reproductive organs of the patient, thereby rendering them sterile. Again, some patients, providers, and institutions choose not to participate in these interventions because of their ethical, moral, or religious values.

Just as the beginning of life can create ethical situations, so can end-of-life decisions. For terminally ill patients, quality of life becomes an important consideration. Patients and families often have to decide whether to continue treatment, which may be difficult for the patient to endure, or to forgo treatment for the duration of the patient's life. Advancements in healthcare treatments have created an even more difficult paradigm of decision making as providers are able to offer more interventions that may increase life span for terminally ill patients. When no cure is possible, patients and families must decide when quality of life surpasses quantity of life; or when the quality of days is more important than the number of days remaining for their loved one. Many who choose quality of life over quantity opt for hospice care. **Hospice care** is palliative care provided to terminally ill patients, often in their home or residential living facility. Other options for end-of-life treatment and procedures may be available in particular states where voluntary euthanasia, or physician-assisted suicide, is legal.

Decisions regarding end-of-life matters are often dealt with through legal determinations, although these decisions remain incredibly difficult and many patients and families struggle with the ethical obligations involved. Family wishes and patient wishes are sometimes not synonymous. During a period of life where emotions are already high, creating an environment conducive to decision making is key. Providing useful information, access to resources and time can assist families in this process. A patient's right to self-determine care or not receive care as well as legal issues surrounding life decisions are discussed in chapter 8.

Genetics, Genetic Testing, and Gene Therapy

Contemporary medicine has advanced such that an individual's genetic code can be examined, and predictions of disease incidence can be made based on the content of that code. An individual's decision to discover those predictions is personal, but it may raise ethical issues between the individual and family members. For example, a patient with a family history of breast or ovarian cancer may undergo genetic testing to determine his or her likelihood of developing the disease. Some patients who discover they are carrying the *BRCA1* gene are at a higher risk of developing the disease, and thus, decide to have preventative procedures performed, such as removing their breasts or ovaries (Metcalfe et al. 2013). Others argue that genetic testing results in prediction of disease rather than certainty, and organ removal may not be the best course of action for an individual. Test results should not automatically result in major surgical procedures; however, more frequent screenings may be a better option (Veeravagu 2015).

Genetic testing can be done on couples to determine the likelihood of certain genetic diseases in their offspring, and the results may lead to ethical questions of whether to reproduce. Also, testing can be done on fetuses in utero. Discovering that a fetus has a particular genetic disorder may create ethical decisions to be made by the parents. Finally, gene therapy is an experimental form of gene research that is still being developed with limited use. Gene therapy involves identifying mutated genes in a patient's DNA and replacing the mutated gene with a healthy copy of the gene. Although risky, promising results have provided encouragement for continued study. However, altering an individual's genetic identity is a fiercely debated intervention and one that results in ethical, moral, religious, and in some cases, political concerns (Terry 2017, 470).

With advancements in genetic testing and treatment, more genetic information is generated. This information is considered sensitive and poses a challenge for HIM professionals to properly store, secure, and transmit such information. The Genetic Information Nondisclosure Act of 2008 (GINA) was passed to regulate the use and disclosure of genetic information specifically. GINA also created new regulations related to the use of genetic information in determination of life and health insurance. Overall, GINA prevents misuse of genetic information and provides patients with certainty of the protection of their information (Asmonga 2008).

Ethical Decision Making in HIM and Informatics

Healthcare clinicians, providers, and staff may face ethical decisions daily regarding the care provided to a patient and the patient's well-being. Ethical decisions made by HIM and informatics professionals differ from those of caregivers in that the decisions of the former are related to managing the patient's health data or information rather than their care. For example, in revenue management, coding has a direct effect on reimbursement. Concerns may arise related to assignment of correct codes and pressure to maximize reimbursement, which may result in a higher level of payment. A HIM department director with knowledge of regulatory coding rules and strong ethical judgment will manage the coding process to ensure validity of codes and correct payment, thus preventing healthcare fraud and abuse. Inquiries made to physicians for clarification can assist coders in their decisions while also enhancing the quality of the documentation in the record.

Although patients and healthcare providers or professionals may face different ethical issues, their decisions often require information or access to patient information. Maintaining patient information, anticipating patient information needs, and granting access to this information can assist patients in their decision-making process. Advancements in technology have also revolutionized the amount of data collected as well as how data is stored, shared, accessed, and disclosed. Ethical issues related to the use and protection of patient information are surfacing as a result of the increased use of electronic health records (EHRs) and biomedical data sources. Integration of medical devices and inclusion of their data creates ethical concerns related to "(1) accurate collecting and reporting of data by the devices; (2) the ability of consumers to understand the data that is presented, as well as a mechanism to ensure that consumers will not misinterpret the data; and (3) integrating the data reliably and accurately with the EHR to inform clinical decision making" (Fenton and Cornelius 2017, 378).

The challenge for health information management and informatics professionals is to work with appropriate organizational staff to ensure policies and procedures are in place when ethical issues arise.

Check Your Understanding 2.3

Instructions: Indicate whether the following statements are true or false (T or F).

1. Taking a step-by-step approach to ethical decision making can assist an HIM or informatics professional when faced with a challenging decision.
2. Stem cell research is an example of a bioethical issue.
3. GINA is an ethical code used to establish expected responses to conflicts of interest.
4. When making an ethical decision, the first step is to gather the applicable facts.
5. Ethics committees create internal recommendations for ethical decisions.

Jan Geisler is the HIM director at Hillside Medical Center. The administration at Hillside has just approved the budget, which includes a new electronic health record. They assigned Jan as the project manager and give her the task of reviewing and selecting the company (vendor) with the EHR that best suits the hospital's needs. Jan immediately thinks of her college roommate, Ana. Ana also majored in HIM and now works for a large EHR vendor in California. Jan sends a quick e-mail to Ana to catch up and asks about her company's EHR system. Ana responds immediately with updated

(Continued)

pictures of her family and some general information about the EHR her company sells. Ana offers for her company to fly Jan to California so she can see the system and have a live demonstration. As an added bonus, Ana writes that she cannot wait to see her friend, take her to dinner, and catch up. Jan goes to California and enjoys her time with Ana, but she is a little disappointed with the EHR system. She just doesn't think it will meet the needs of her hospital. Jan has a meeting with the chief information officer today and is expected to present her recommendations. She feels obligated to recommend Ana's company, but she also has major concerns about their product.

What ethical issues can be found in Ana's investigation of EHRs?

Was it a conflict of interest for Jan to do business with her personal friend Ana?

Using the ethical decision-making model described in this chapter, analyze the scenario and recommend a decision.

References

AHIMA. 2011a. Code of ethics. http://www.ahima.org.

AHIMA. 2011b. AHIMA Consumer Health Information Bill of Rights: A Model for Protecting Health Information Principles. http://www.ahima.org.

Allen, James F. 2013. *Health Law and Medical Ethics for Healthcare Professionals*. Boston: Pearson.

American Medical Association. 2007. E-history. http://www.ama-assn.org.

American Medical Association. 2016. Code of Medical Ethics. https://www.ama-assn.org/about-us/code-medical-ethics.

American Medical Informatics Association. 2010. Strategic Alignment Summary. http://www.amia.org.

American Medical Informatics Association. 2013. Code of professional ethical conduct. http://www.amia.org

Asmonga, D.D. Getting to know GINA: An overview of the Genetic Information Nondiscrimination Act. *Journal of AHIMA* 79(7):18, 20, 22.

Beauchamp, T. and J. Childress. 2012. *Principles of Biomedical Ethics*, 7th ed. New York: Oxford University Press.

Blanchard, K. and N.V. Peale. 1988. *The Power of Ethical Management*. New York: William Morrow.

Brotherton, S., A. Kao, and B.J. Crigger. 2016. Professing the values of medicine: The modernized AMA Code of Medical Ethics. *JAMA,* 316(10):1041–1042. doi:10.1001/jama.2016.9752

Crawford, M. 2011. Everyday ethics. AHIMA code of ethics guides daily work, complex situations. *Journal of AHIMA* 82(4):30–33.

Ethics & Compliance Initiative. n.d. Ethics & compliance toolkit. https://www.ethics.org/resources/free-toolkit.

Fenton, S. and F. Cornelius. 2017. *Ethical Health Informatics: Challenges and Opportunities*, 3rd ed. Edited by Harman, L. and F. Cornelius. Sudbury, MA: Jones and Bartlett Learning.

Fremgen, B. 2016. Medical Law and Ethics. 5th ed. Boston: Pearson.

Glover, J. 2017. Ethical Decision-Making Guidelines and Tools. *Ethical Health Informatics Challenges and Opportunities*, 3rd ed. Edited by Harman, L. and F. Cornelius. Sudbury, MA: Jones and Bartlett Learning.

Hurst, S., S. Hull, G. DuVal, and M. Danis. 2005. How physicians face ethical difficulties: A qualitative analysis. *Journal of Medical Ethics* 31(1):7–14. http://doi.org/10.1136/jme.2003.005835.

Judicial Council. 1985. Guidelines for ethics committees in healthcare institutions. *JAMA* 253(18):2698–2699.

Khushf, G. 2004. Handbook of bioethics: Taking stock of the field from a philosophical perspective. Boston: Kluwer Academic.

Kirk, L. 2007. Professionalism in medicine: Definitions and considerations for teaching. *Proceedings (Baylor University Medical Center)*. 20(1):13–16.

Maslow, A.H. (1943). A theory of human motivation. *Psychological Review* 50(4):370–396.

Metcalfe, K., C. Kim-Sing, P. Ghadirian, P. Sun, and S. Narod. 2013. Health care provider recommendations for reducing cancer risks among women with a *BRCA1* or *BRCA2* mutation. *Clinical Genetics,* 85(1):21–30.

Neuberger, B. J. and E.S. Swirsky. 2017. Public health and informatics. In *Ethical Health Informatics: Challenges and Opportunities*, 3rd ed. Edited by Harmen, L. and F. Cornelius. Sudbury, MA: Jones and Bartlett Learning.

Science Reference Services. 2015. Bioethics Tracer Bullet 91-4. http://www.loc.gov/rr/scitech/tracer-bullets/bioethicstb.html.

Terry, S. 2017. Genetic Information. In *Ethical Health Informatics: Challenges and Opportunities*, 3rd ed. Edited by Harmen, L. and F. Cornelius. Sudbury, MA: Jones and Bartlett Learning.

The Joint Commission International Accreditation Standards for Hospitals, 5th ed. Standards GLD.12, GLD.12.1, GLD.12.2. https://www.ethics.org/eci/research/free-toolkit/decision-making-model#filters.

Veeravagu, A. 2015. Why Angelina Jolie's Surgery Isn't for Everyone. *The Daily Beast*. http://www.thedailybeast.com/articles/2015/03/24/why-angelina-jolie-s-surgery-isn-t-for-everyone.html.

Cases, Statutes, and Regulations Cited

Davis v. Davis, 842 S.W.2d 588 (Tenn. Supr. 1992).

In re Quinlan, 70 N.J. 10, 355 A.2d 647 (1976).

Louisiana Code of Governmental Ethics, R.S. 42:1111–1121, Section III, F 1112.