FORDNEY'S MEDICAL INSURANCE AND BILLING

16TH EDITION

LINDA M. SMITH

ELSEVIER

Evolve®

Student Resources on Evolve
Access Code Inside

Evolve®

YOU'VE JUST PURCHASED MORE THAN A TEXTBOOK!

Enhance your learning with Evolve Student Resources.

These online study tools and exercises can help deepen your understanding of textbook content so you can be more prepared for class, perform better on exams, and succeed in your course.

Activate the complete learning experience that comes with each NEW textbook purchase by registering with your scratch-off access code at

http://evolve.elsevier.com/Smith/Fordneys/

If your school uses its own Learning Management System, your resources may be delivered on that platform. Consult with your instructor.

If you rented or purchased a used book and the scratch-off code at right has already been revealed, the code may have been used and cannot be re-used for registration. To purchase a new code to access these valuable study resources, simply follow the link above.

Place Sticker Here

REGISTER TODAY!

ELSEVIER

You can now purchase Elsevier products on Evolve!
Go to evolve.elsevier.com/shop to search and browse for products.

2019v1.0


FORDNEY'S
MEDICAL
INSURANCE
AND BILLING

FORDNEY'S MEDICAL INSURANCE AND BILLING

16TH EDITION

LINDA M. SMITH
CPC, CPC-I, CEMC, CMBS
Training and Consulting
MedOffice Resources
Greene, New York

ELSEVIER

Elsevier
3251 Riverport Lane
St. Louis, Missouri 63043

FORDNEY'S MEDICAL INSURANCE AND BILLING, SIXTEENTH EDITION

ISBN: 978-0-323-79535-7

Library of Congress Control Number: 2021946514

Senior Content Strategist: Linda Woodard
Content Development Specialist: Brooke Kannady
Director, Content Development: Laurie Gower
Publishing Services Manager: Shereen Jameel
Senior Project Manager: Umarani Natarajan
Design Direction: Amy L. Buxton

Printed in India

Last digit is the print number: 9 8 7 6 5 4 3 2 1

ABOUT THE AUTHOR

Linda M. Smith has worked in the health care industry for more than 40 years. She started her career as a medical assistant and journeyed through the health care industry, spending time in various positions. Throughout that time, the health care industry went through dramatic changes. Health care providers experienced a multitude of billing and reimbursement changes, while also facing the challenges of an ever-increasing focus on regulatory guidelines and compliance. Simultaneously, the need for trained staff and resources to assist with billing, reimbursement, and compliance issues increased, which led her to found her own company, MedOffice Resources, in 2000. MedOffice Resources provides training to health care organizations and to various business and technical schools. She and her associates provide training in the areas of medical ethics, medical terminology, anatomy and physiology, medical coding and billing, and value-based incentive programs. Billing, coding, and auditing services are also offered to health care organizations. Health care facilities, practices, providers, and their office staff have been using the services of MedOffice Resources for the past 20 years to strengthen their staff's skills and strengthen their organizations.

Ms. Smith is a certified professional coder (CPC). She has also earned the credentials E/M coding specialist (CEMC) and is an approved professional medical coding curriculum instructor (CPC-I) through the American Academy of Professional Coders (AAPC). Additionally, Ms. Smith holds the credential of certified medical billing specialist (CMBS) through the Medical Association of Billers.

Ms. Smith was given the opportunity to work with Marilyn Fordney, the original author of the *Insurance Handbook for the Medical Office*. She worked with Fordney as a contributor to the textbook. After Ms. Fordney's retirement, Smith took on the editor position for the 15th and 16th editions.

ACKNOWLEDGMENTS

I would like to acknowledge and dedicate this 16th edition of the *Insurance Handbook* to Marilyn Fordney, the original author of this textbook. Marilyn published the first edition of the *Insurance Handbook* in 1977 and has followed it through the many changes in our health care industry. It has served as the training tool and building block for so many of us in the field. The publication's longevity speaks for itself.

It was a privilege to have been asked to be a contributor in the 13th and 14th editions of the *Handbook*, but an even greater honor to be asked to follow in Marilyn's footsteps as the primary editor of the 15th and 16th editions. Marilyn is a remarkable woman with a beautiful heart. Thank you, Marilyn, for all you have contributed to our field.

I would also like to give special thanks to Cheryl Fassett, who has been an outstanding partner in this project and a contributor in eight chapters of this 16th edition. Cheryl's expertise in our field, coupled with her outstanding talent and love for writing, has made this experience even more enjoyable. Cheryl's work is both remarkable and exemplary. I can't think of anyone else I would rather take this ride with.

And to the former owner of Practicare Medical Management, Hal Harkavy, a sincere thank you for asking me to join you in your journey into the world of outsourced medical billing so many years ago. There is so much that you taught me for which I will always be thankful.

Thank you to the many students who have given me the opportunity to share my knowledge of the medical billing and coding field. I can only hope that you will find the passion for it that will provide you with all the opportunities I have had the pleasure of. You have been my motivation and my reward.

I am indebted to many individuals on the staff at Elsevier for encouragement and guidance. Thank you to all the experts in the field who served as reviewers of the 15th edition and guided us with their recommendations. I express special appreciation to Linda Woodard, senior content strategist, and Brooke Kannady, content development specialist at Elsevier.

And lastly, thank you to my husband, John Wells, and my family who always support and encourage me. You are my reason for everything.

Linda M. Smith, CPC, CPC-I, CEMC, CMBS

CONTRIBUTOR AND REVIEWERS

CONTRIBUTOR

Cheryl Fassett, CPC, CPMA, CRC, CDEO, CPB, CPPM, CPC-I
Practice Manager
Riverside Associates in Anesthesia, PC
Binghamton, New York

REVIEWERS

Christine L. Berard, CPT
Coordinator/Instructor
Medical Billing & Coding, 911Programs
Warwick, Rhode Island

Rita Courier, MA, CCA
Account Representative/Billing & Coding Instructor
Hospital Community College
Munson Healthcare Otsego Memorial Hospital
North Central Michigan Community College
Gaylord, Michigan, Petoskey, Michigan

Nadinia Davis, MBA, RHIA, CHDA, FAHIMA
Adjunct Instructor
Delaware Technical Community College
Wilmington, Delaware

Melissa De Leon, NRCCS, NRCAHA
Medical Coding and Billing Program Director
Medical Office Specialist Program Director
The College of Health Care Professions
McAllen, Texas

Nancy J. Gammons, MS, CCS-P, CHSP, CHLP
AHIMA-approved ICD-10-CM/PCS Trainer
Certified Coding Specialist—Physician Based
Certified HIPAA Security Professional
Certified Health IT Leadership Proficiency
Professor HIT Programs
Allied Health Department
Shawnee Community College
Ullin, Illinois

Sandra J. Hertkorn, UC Davis Coder Academy
Director of Operations
Administration
All Inclusive Medical Services
Adult Ambulatory Clinic
Carmichael, California

Jennifer K. Jones, CPC, CPC-I, OHCC, CCS, CPMA
Columbia, Alabama

WELCOME TO THE 16TH EDITION

This textbook was first published by Marilyn Fordney as the *Insurance Handbook* in 1977. At that time, few people were aware of how important the subject of health insurance would become. I am confident that Marilyn Fordney had no idea that her textbook would become the basis of knowledge for so many of us in the field. Marilyn Fordney is a dedicated professional and a forward thinker whose work provided a strong foundation to many of us entering the field.

Forty-four years after that first publication, the textbook is celebrating its 16th edition. The longevity of this publication speaks for itself, and through the years, Fordney's textbook has been the leader in its field. The textbook is widely accepted across the nation among educators and those working in the health care industry.

Originally, the *Insurance Handbook* was designed primarily for students who planned to seek employment in the outpatient setting (such as a physician's office or clinic). The name of the publication was changed to *Fordney's Medical Insurance and Billing* at the 15th edition of the textbook and changes were made to expand the textbook beyond the world of professional billing and into facility billing. With this expansion, the textbook now provides a strong foundation to students who may also seek employment in a hospital, nursing home, or other type of health care facility.

To remain at the forefront of the industry and because of the ever-changing nature of health care, *Fordney's Medical Insurance and Billing* is revised every 2 years to keep the information current. Reviewing and revising the 16th edition has been as challenging and exciting as all of the publications before it.

PURPOSE

The goals of this textbook are to prepare students to excel as insurance billing specialists and to increase efficiency and streamline administrative procedures for one of the most complex tasks of the health care industry: insurance coding and billing.

Why Is This Book Important to the Profession?

In the past several decades, health care professionals and the community have witnessed the emergence of an administrative medical specialty known variously as insurance billing specialist, medical biller, or reimbursement specialist. Thus *Fordney's Medical Insurance and Billing* has been written to address the specialty of medical billing as another branch of the administrative medical assistant profession.

As the complexity of the health care field increased, the need for both basic and advanced training has become essential. There are national organizations offering certification in the field, which has quickly become the method of attaining higher recognition for advanced skill levels. *Fordney's Medical Insurance and Billing* will serve as a training tool to establish a strong foundation of knowledge and will help bridge the learning process into the more advanced levels of expertise.

Insurance claims are being submitted for patients on the recommendation of management consultants to control cash flow, obtain correct reimbursement amounts, honor insurance contracts, compete with other health care organizations, and maintain a good relationship with patients. Even health care organizations that do not routinely complete insurance claims for patients make exceptions for elderly patients or patients with mental incompetence, illiteracy, diminished eyesight, or a poor command of the English language. When the amount of the bill is hundreds or thousands of dollars or when a surgical report is required, the health care organization should submit the bill to obtain maximum reimbursement. Individuals who administer the federal government's Medicare program increasingly promote electronic transmission of insurance claims for medium-sized and large medical practices. Because of these factors, as well as federal mandates to document care electronically, the amount of knowledge and skills that one must have has substantially increased. This textbook addresses all clerical functions of the insurance billing specialist, and illustrations throughout the text feature generic forms created to help simplify billing procedures.

Who Will Benefit From This Book?

Many colleges are now offering associate degree programs in medical billing and coding. At the same time, schools and colleges also offer 1-year certificate programs for those interested in a career as an insurance billing specialist. The student may find programs that offer medical insurance as a full-semester, 18-week course on campus or as a hybrid course (mix of online and face-to-face classroom instruction). Some schools include medical billing and coding as part of a medical assisting program's curriculum, so the individual has knowledge in all administrative functions of a health care organization. *Fordney's Medical Insurance and Billing* may be used as a learning tool and resource guide in all of those programs as well as in vocational or commercial training institutes. *Fordney's Medical Insurance and Billing* is recommended for use as a text for in-service training in health care organizations or it can be used for independent home study if no formal classes are available in the community. The layperson who is not pursuing a career in the medical field will find the textbook useful when working with a claims assistance professional or for billing his or her insurance plans. Insurance companies and their agents have found *Fordney's Medical Insurance and Billing* to be a valuable reference tool when answering clients' questions. Finally, the textbook may be used as a stand-alone reference source or as an educational tool to increase the knowledge of someone currently working as an insurance billing specialist in any health care setting.

CONTENT

General Features

Each chapter has been updated to reflect current policies and procedures.

- All chapters have been completely restructured for better organization and flow of content, with legal information included where applicable to insurance billing and coding. The information presented is not a substitute for legal advice, and the health care organization and their insurance billing specialists should always seek legal counsel about specific questions of law as they relate to their organization.

The unique color-coded icons have been visually updated and are featured throughout the textbook to denote and clarify information specific to each type of payer. This system makes the learning process more effective by helping students to identify each insurance payer with a specific color and graphic. These icons follow:

COMPLIANCE ALERT

- Compliance Alerts are interspersed throughout all chapters for emphasis.
- Objectives are provided at the beginning of each chapter, sequenced to match the technical content, and help to guide instructors in preparing lecture material and inform readers about what material is presented.
- By reviewing the key terms that introduce each chapter, students are alerted to important words for the topic. Key abbreviations follow the key terms; spell-outs of the abbreviations are provided in a section that follows the Glossary near the back of the textbook.
- Boxed examples are provided throughout each chapter.
- Key points are presented at the end of each chapter, summarizing and emphasizing the most important technical information in the chapter.

Many experts in the field reviewed the chapters in previous editions so that improvements in content, clarity of topics, and deletions could be considered.

INSIGHTS FROM THE FIELD

- Each chapter includes "Insights From the Field," which is a short interview with an insurance billing specialist with experience in the field, who provides a snapshot of their career path and advice to the new student.

QUICK REVIEW QUESTIONS

- Quick review questions have been added within each chapter to facilitate learning of key points.

DISCUSSION POINTS

- Discussion points at the end of each chapter will provide the opportunity for students and instructors to participate in interesting and open dialogue related to information provided.

PRIVATE INSURANCE

The Blue plans and private insurance.

MANAGED CARE

All managed care organizations.

MEDICARE

Federal Medicare programs, Medicare/Medicaid, Medicare/Medigap, and Medicare Secondary Payer (MSP).

MEDICAID

State Medicaid programs.

MILITARY PLANS

TRICARE plans and the Civilian Health and Medical Program of the Department of Veterans Affairs.

WORKERS' COMPENSATION

State workers' compensation programs.

ORGANIZATION

Unit 1: Career Role and Responsibilities

- Chapters 1 through 3 are included under Unit 1, Career Role and Responsibilities, which explains the role of the insurance billing specialist and provides the student with a thorough understanding of the associated responsibilities. Because of the strong base of knowledge that the insurance billing specialist will need to understand the federal and state guidelines associated with the industry, Chapters 2 and 3 have in-depth information surrounding privacy, security, and health care fraud and abuse legislation. This is coupled with a strong emphasis on the compliance process and the insurance billing specialist's obligation to comply in all situations.

Unit 2: Introduction to Health Insurance

- Chapters 4 through 10 make up Unit 2, Introduction to Health Insurance. This unit will provide the student with an introduction into health insurance. The chapters in this unit are intended to build the learners' foundation of the basics of health care and introduce them to the various types of insurance carriers they will most likely encounter. Thorough, up-to-date information is presented for Medicare, Medicaid, TRICARE, private plans, workers' compensation, managed care plans, disability income insurance, and disability benefit programs.

Unit 3: Documentation and Coding for Professional Services

- Chapters 11 to 13 are included under Unit 3, Documentation and Coding for Professional Services. Medical

documentation and the electronic health record have become essential components of the medical billing process. The insurance billing specialist must be knowledgeable of federal and industry-wide documentation requirements to assist providers and to ensure compliance in billing. Furthermore, the student will learn and develop diagnostic coding and procedural coding skills.

Unit 4: Claims Submission in the Medical Office

- Chapters 14 and 15 make up Unit 4 and will teach students the claims submission process. The textbook offers a unique block-by-block approach for completion of a paper insurance claim form in Chapter 14. In Chapter 15, the student will learn the electronic claims process and the advantages of electronic claim submission. They will learn federal legislation that governs the electronic claims process and the standard requirements for electronic claims submission.

Unit 5: Revenue Cycle Management

- Unit 5 is titled Revenue Cycle Management and includes Chapters 16 and 17. These chapters focus on the skills necessary to receive and process payments for health care services. Chapter 16 provides problem-solving techniques to use when dealing with insurance carriers. Chapter 17 provides the student with office and insurance collection strategies.

Unit 6: Health Care Facility Billing

- Chapter 18, Introduction to Health Facilities and Ambulatory Surgery Centers, was renamed in the 16th edition and expanded to introduce the student to many types of health care facilities they may be associated with throughout their career. The chapter describes the different types of health care facilities, rules, and guidelines specific to facility billing and the many types of reimbursement systems that health care facilities work with. Chapter 19, Billing for Health Care Facilities, was also renamed in the 16th edition. This chapter now outlines the billing process used by health care facilities and claim form completion. Furthermore, the chapter presents coding guidelines specific to facility billing and information about the *International Classification of Disease, Tenth Revision, Procedure Classification System (ICD-10-PCS)*. Step-by-step procedures are stated for processing a new patient for admission and to verify insurance benefits. Both Chapters 18 and 19 have been updated to provide the most current issues impacting insurance billing specialists in the facility setting.

Unit 7: Employment

- Chapter 20, Seeking a Job and Attaining Professional Advancement, provides insight into the insurance billing career field and lists employment opportunities for those seeking a position after their training. The chapter covers the job search, application, and interview processes. Information regarding advanced job opportunities, certification and the importance of professional organizations, networking, and mentoring are offered.

ANCILLARIES

Workbook

For students, the *Workbook* that accompanies the textbook is a practical approach to learning insurance billing. It progresses from easy to more complex issues within each chapter and advances as new skills are learned and integrated.

The *Workbook* that accompanies this edition of the textbook contains the following features:

- Each chapter has performance objectives for assignments that indicate to students what will be accomplished.
- Key terms are repeated for quick reference when studying.
- Key abbreviations followed by blank lines are listed alphabetically so that students can assemble their own reference list for each chapter, thus reinforcing the abbreviations' spell-outs.
- Assignments which include fill-in-the-blank, multiple-choice, mix-and-match, and true/false review questions.
- Some assignments give students hands-on experience in completing insurance claims on the CMS-1500 and UB-04 claim forms using standardized guidelines.
- Patients' medical records, financial accounting statements, and encounter forms are presented as they might appear in the health care organization's files so that students may learn how to abstract information to complete claim forms properly and accurately.
- Patient records and ledgers have been completely updated for technical clinical content and reworded to correspond with the 2021 CPT procedural and ICD-10-CM diagnostic code books.
- Easily removable forms and other sample documents are included in the *Workbook* for completion and to enhance keying skills.
- A final test section at the end of the *Workbook* to provide a complete, competency-based educational program.
- Answers to *Workbook* assignments have been put into the Instructor Resources that are available on the companion Evolve website.

Special appendixes are included at the end of the *Workbook*. These include a simulated practice, the College Clinic, with a group of physicians who employ the student. The appendix may be used as reference tools to complete workbook problems. These appendixes include the following:

- Appendix A details information for a simulated practice called *College Clinic*. Information is provided about the group of physicians and a mock fee schedule is included with codes and fees (including Medicare).

Evolve Companion Website (for Instructors)

Evolve is an interactive learning environment that works in coordination with the textbook. It provides internet-based course management tools that instructors can use to reinforce and expand on the concepts delivered in class. It can be used for the following:

- To publish the class syllabus, outline, and lecture notes
- To set up "virtual office hours" and e-mail communication

- To share important dates and information through the online class calendar
- To encourage student participation through chat rooms and discussion boards

The *TEACH Instructor's Resource Manual* is also available on the Evolve site. This resource allows instructors the flexibility to quickly adapt the textbook for their individual classroom needs and to gauge students' understanding. The *TEACH Instructor's Resource Manual* features the following:

- Announcements and content updates that become available.
- Lesson plans for each chapter.
- Power point slides and handouts for each chapter.
- Answer keys to the *Workbook* and Student Software Challenge assignments and tests with rationales, optional codes, and further explanations for most of the code problems
- Test banks for each chapter.

Evolve Companion Website (for Students)

Evolve also provides online access to free Learning Resources designed specifically to give students the information they need to quickly and successfully learn the topics covered in this textbook. These Learning Resources include the following:

- Announcements and content updates that become available.
- Blank CMS-1500 claim forms with the instructions for completion by the National Uniform Claims Committee (NUCC).
- Blank UB-04 claim forms with guidance for completion of both paper and electronic claims.
- Student 1500 Software Challenge simulates realistic experience by having students gather necessary documents and extract specific information to complete the CMS-1500 insurance claim form.
- Performance Evaluation Checklists for each chapter.
- Self-assessment quizzes and final exam to evaluate students' mastery through multiple-choice, true/false, fill-in-the-blank, and matching questions. Instant scoring and feedback are available at the click of a button.

Medical Insurance Online for Fordney's Medical Insurance and Billing

Medical Insurance Online for Fordney's Medical Insurance and Billing provides supplementary content and engaging activities to help students master the information presented in *Fordney's Medical Insurance and Billing, 16e.* Gradable case studies and assessments measure student progress and comprehension of the essential and challenging concepts that health insurance professionals face in the industry today. This course meets 508 and WCAG 2.0 accessibility criteria.

SUMMARY

Fordney's Medical Insurance and Billing and its ancillaries provide a complete competency-based educational program. The textbook and workbook learning and performance objectives, assignments, tests, Student Software Challenge, and incorporation of lesson plans and suggested classroom activities from the *TEACH Instructor's Resource Manual* ensure that students know everything they need to succeed in the workforce. Escalating costs of medical care, the effect of technology, and the multitude of insurance types have affected insurance billing procedures and claims processing and have necessitated new legislation for government and state programs. Therefore, it is essential that all medical personnel who handle claims continually update their knowledge. This may be accomplished by reading bulletins from state agencies and regional insurance carriers, speaking with insurance representatives, or attending insurance workshops offered at local colleges or local chapters of professional associations, such as those mentioned in Chapters 1 and 20. It is hoped that this textbook will resolve any unclear issues pertaining to current methods and become the framework on which the insurance billing specialist builds new knowledge as understanding and appreciation of the profession are attained.

Linda M. Smith, CPC, CPC-I, CEMC, CMBS
Greene, New York

CONTENTS

UNIT 1

Career Role and Responsibilities

1

Role of an Insurance Billing Specialist

Linda M. Smith

OBJECTIVES

After reading this chapter, you should be able to:

1. Identify the background and importance of accurate insurance claims submission, coding, and billing.
2. Assess the various roles and responsibilities assigned to insurance billing specialists.
3. Name and discuss the office procedures performed in a health care organization during a workday that may affect billing.
4. Specify the educational requirements for a job as an insurance billing specialist and a coder.
5. Describe the variety of career advantages open to those trained as insurance billing specialists.
6. List qualifications, attributes, and skills necessary to be an insurance billing specialist.
7. Determine an appropriate dress code that would provide an image of confidence and professionalism.
8. Describe professional behavior when working as an insurance billing specialist.
9. Differentiate between professional ethics and medical etiquette.
10. Specify instances when an employer, an employee, or an independent contractor can be liable when billing for medical services.
11. Identify common practices and limitations of a claims assistance professional's scope of practice to his or her clients.
12. Explain how insurance knowledge and medical knowledge can be kept current.

KEY TERMS

accounts receivable
American Medical Association
cash flow
claims assistance professional
claims examiners
cycle
dress code
electronic mail
emoticons
encounter
errors and omissions insurance
ethics
etiquette
facility billing
health record
independent contractor
insurance billing specialist
management service organizations
medical billing representative
medical record
non-physician practitioner
personal health record
physician extender
professional billing
professional liability insurance
reimbursement specialist
respondeat superior
revenue
self-pay patient
senior billing representative
text speak

KEY ABBREVIATIONS

AMA
ASHD
CAP
e-mail
MSO
NPP

INSIGHTS FROM THE FIELD

Melissa A.: Certified Professional Coder (CPC) and Billing/Coding Consultant

I started into health care 36 years ago, as a transport specialist. From there I worked as a phlebotomist, operating room scheduling secretary, and medical office assistant where I learned medical billing and became very proficient at it. I went on to get my coding certification and all of this led me to where I am today. Currently, I am employed by a large health care organization where I perform coding for their skilled nursing facility. I also provide consulting services to medical practices. In my opinion, the most valuable skills an individual can have in this field are perseverance and determination. It's my job to bring the money in. I have always taken my role very personally whether I was working for a private practice or a large organization. If I am not successful in my role, the health care organization may not survive.

BACKGROUND OF INSURANCE CLAIMS, CODING, AND BILLING

Welcome to the world of medical billing, an exciting, ever-changing, and fast-growing career field. To help focus on important terms and definitions, the key words in this and subsequent chapters appear in **bold** or *italic* type.

Insurance billing specialists are nonclinical medical staff who work in all types of health care organizations. Their primary goals are to help patients obtain maximum insurance plan benefits for the services they received while ensuring the cash flow of their organization through revenue cycle management. **Revenue** is the total income produced by a medical practice or health care organization, and the **cycle** is the regularly repeating set of events for producing it.

Over the years, medical billing has become extraordinarily complex. The charge for a baby being born in the late 1960s could have been as little as $250. This was a flat fee that covered a 3-day hospital stay and a doctor's fee. The receipt for the birth typically looked like a receipt from a hardware store and contained the name of the patient, the total cost of care, and three options for payment (cash, check, or money order). Today, the average cost for giving birth is estimated to be between $5000 and $11,000 for an uncomplicated vaginal delivery. The estimated average cost for a cesarean birth can range from $7500 to $14,500 while complications during birth may further increase the charge. These prices include the total duration of care, the obstetrician's fee, the anesthesiologist's fee, and the hospital care fee. And as the charge for services has increased, so has the complexity of billing for them. There are numerous payers that the billing specialist must be familiar with, each with their own guidelines. In addition, health care organizations use electronic medical records, electronic health records, and personal health records which the insurance billing specialist must be familiar with and learn to use.

- **Medical records** refer to patient charts which includes notes and information collected by and for the clinicians in that specific health care provider's office or organization.
- **Health records** refer to information collected from *all* of the clinicians involved in a patient's care. Clinicians can be authorized to access the patient's health record to assist them in providing care to that patient. Health records could include such things as laboratory and radiology reports or consultations with other providers.
- **Personal health records** are designed to be set up, accessed, and managed by the patient. The records typically contain information such as diagnoses, medications, immunizations, family medical histories, and provider contact information.

The insurance billing specialist must also have strong computer skills and learn to use the various software programs used for medical billing. Patient conditions and services must be coded which is a skill that individuals must excel in. Additionally, there are various methods of reimbursement for the services that the insurance billing specialist must be familiar with. It is often difficult for health care organizations to obtain maximum payment for services. The health care industry is one of the most heavily regulated industries in the United States. There are laws that must be followed and many billing and coding guidelines. Physicians and health care organizations rely on professional insurance billing specialists to handle this complex part of their business. An insurance billing specialist must be knowledgeable of the health care system and all of the components, interrelationships, and interdependencies, such as hospitals, outpatient laboratories, insurance companies, federal government, patients, patient families, other health care professionals, and co-workers.

In medical billing, there are two different types of billing: facility billing and professional billing. **Facility billing** is charging for services done in hospitals, acute care hospitals, skilled nursing or long-term care facilities, rehabilitation centers, or ambulatory surgical centers. **Professional billing** is charging for services performed by physicians or **non-physician practitioners (NPPs)**. An NPP is a provider of health care services, such as a physician assistant, nurse practitioner, advanced registered nurse practitioner, certified nurse anesthetist, physical therapist, speech therapist, licensed clinical social worker, or certified registered nurse practitioner, who has not obtained a medical degree but is allowed to see patients and prescribe medications. These professionals are sometimes referred to as **physician extenders**. Professional billing is also relevant to other ancillary providers such as ambulance services, radiology and laboratory services, and physical therapists. This textbook will address both facility billing and professional billing. Although there are significant differences in the processing of claims between facility and professional billing, the basic setup of a business office encompasses the following units or combined departments:

- reception of the patient,
- rendering of medical services,
- documentation of the services, and
- financial accounting.

The insurance billing specialist must understand the function of each department in relation to the business office and the health care organization as a whole and how they affect the revenue cycle. The flow of information between departments is one of the most vital components of an organization.

In the health care organization, office procedures performed throughout a workday include the following:

- *Scheduling appointments* involves assigning time slots for patient encounters. An **encounter** is defined as an interaction between a patient and a health care provider for the purpose of providing health care services or assessing the patient's health

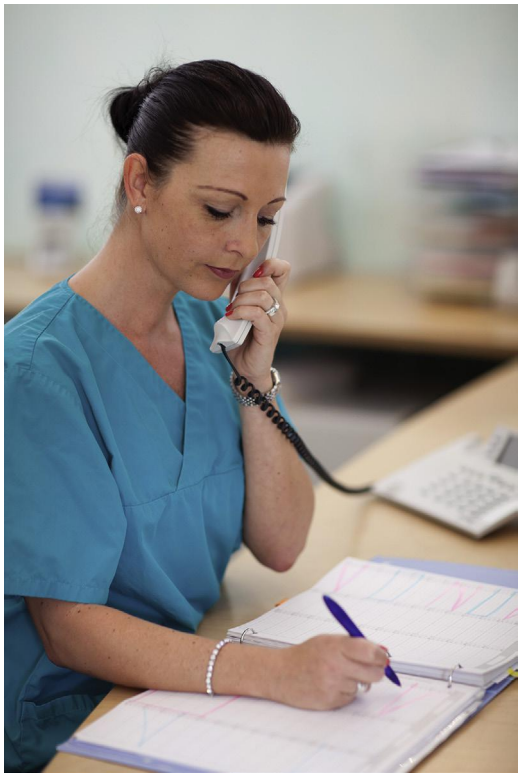

Fig. 1.1 Health care staff scheduling an appointment. (Copyright © iStock.com/fotografixx.)

status. Canceling and rescheduling may also be involved. If the time is not properly assigned, there may be an influx or low volume of patients at a given time. Paperwork required for the encounter must also be produced. It is important to record why the patient requires health care services. See Fig. 1.1.

- *Registering patients* may involve preregistration for visits by using a questionnaire referred to as a *patient registration form.* Financial and personal data are collected and accurately recorded (input) in a timely manner. Incorrect information affects the submission and payment of claims.
- *Documenting* pertinent clinical notes for assignment of a diagnosis and service code to the patient's encounter is done by the provider of service. The notes in the patient's **medical record** include the reason for the encounter, history, physical examination, diagnostic tests, results, diagnosis, and plan of treatment. The insurance billing specialist may be required to contact the insurance company to obtain authorization for treatment by secondary providers. He or she must also ensure that forms are properly completed, and data are input into the system. Both proper documentation and assignment of the correct code for service affect the revenue cycle.
- Posting (inputting) a *charge entry* for patient care service rendered into the billing system by the charge entry staff member. The insurance biller must make certain that the insurance is correct in the system and must ensure that the diagnosis coincides with the service rendered. For example, an obstetrics/gynecology encounter should not have a diagnosis related to ophthalmology. Many times, individuals have the same names, so billing service dates and the name of the patient seen must be accurate. The charge entry staff member must ensure that the correct charge is assigned to the correct patient. Proper charge entry ensures timely billing and reimbursement.
- *Bookkeeping and accounting* is the posting of payments received (cash, checks, electronic funds transfer, or debit and credit cards) to patients' financial accounts. The bookkeeper or accountant must pay special attention to adjustments, denials, and write-offs. These entries may require investigation for validation. He or she may also receive insurance payer remittance advices and may be assigned to follow up on denials.

1.1 QUICK REVIEW
Question: What is the difference between facility billing and professional billing?

ROLE OF THE INSURANCE BILLING SPECIALIST

Several job titles are associated with medical billing personnel. The professional title used may depend on the region within the United States. Some of the most popular titles include insurance billing specialist, electronic claims processor, medical biller, **reimbursement specialist**, **medical billing representative**, and **senior billing representative**. In large health care organizations it is common to find a billing department made up of many people; within the department, each position is specialized, such as Medicare billing specialist, Medicaid billing specialist, coding specialist, insurance counselor, collection manager, and revenue cycle manager. In this handbook the title *insurance billing specialist* will be used throughout to represent this broad spectrum of titles.

Insurance carriers also employ insurance billing specialists who may serve as **claims examiners**. Claims examiners are also referred to as claims adjustors or claims representatives. Their role is to analyze and process incoming claims, checking them for validity and determining if the services were reasonable and necessary.

Some health care organizations contract with **management services organizations (MSOs)**, which perform a variety of business functions, such as accounting, billing, coding, clinical documentation improvement, collections, computer support, compliance oversight, legal advice, marketing, payroll, and management expertise. An insurance billing specialist may find a job working for an MSO as a part of this team.

Individuals called **claims assistance professionals (CAPs)** work for the consumer. They help patients organize, file, and negotiate health insurance claims of all types; assist the consumer in obtaining maximum benefits for the health care services they received; and tell the patient how much to pay the health care organization to make sure there is no overpayment. It is possible for someone who has taken a course on insurance billing to function in this role.

Job Responsibilities

Whether employed by a medical practice, a hospital, or other health care organization as an insurance billing specialist, the individual should be able to perform any and all duties related to the business office. All health care staff, regardless as to whether they work in scheduling, registration, charge posting, or accounting, must work together to ensure a strong revenue cycle and appropriate reimbursement. Health care organizations have job descriptions to outline the job duties, skills, and requirements for insurance billing specialists and other related job titles. See Figs. 1.2 and 1.3.

GENERIC JOB DESCRIPTION FOR ENTRY LEVEL INSURANCE BILLING SPECIALIST

Knowledge, skills, and abilities:
1. Minimum education level consists of certificate from 1-year insurance billing course, associate degree, or equivalent in work experience and continuing education.
2. Knowledge of basic medical terminology, anatomy and physiology, diseases, surgeries, medical specialties, and insurance terminology.
3. Ability to operate computer, printer, photocopy, and calculator equipment.
4. Written and oral communication skills including grammar, punctuation, and style.
5. Ability and knowledge to use procedure code books.
6. Ability and knowledge to use diagnostic code books.
7. Knowledge and skill of data entry.
8. Ability to work independently.
9. Certification in billing and/or coding is preferred.

Salary:
Employer would list range of remuneration for the position.

Job responsibilities:	**Performance standards:**
1. Abstracts health information from patient records.	1.1 Uses knowledge of medical terminology, anatomy, diseases, surgeries, and medical specialties. 1.2 Consults reference materials as needed. 1.3 Meets accuracy and production requirements. 1.4 Verifies with physician any vague information for accuracy.
2. Exhibits an understanding of ethical and medicolegal responsibilities related to insurance billing programs.	2.1 Observes policies and procedures related to federal privacy regulations, health records, release of information, retention of records, and statute of limitations for claim submission. 2.2 Meets standards of professional etiquette and ethical conduct. 2.3 Recognizes and reports problems involving fraud, abuse, embezzlement, and forgery to appropriate individuals.
3. Follows employer's policies and procedures.	3.1 Punctual work attendance and is dependable. 3.2 Answers routine inquiries related to account balances and insurance forms submitted.
4. Transmits insurance claims accurately.	4.1 Updates insurance registration and account information. 4.2 Processes payments and posts to accounts accurately. 4.3 Handles correspondence related to insurance claims. 4.4 Reviews encounter forms for accuracy before submission to data entry. 4.5 Inserts data for generating insurance claims accurately. 4.6 Codes procedures and diagnoses accurately. 4.7 Telephones third-party payers with regard to delinquent claims. 4.8 Traces insurance claims. 4.9 Files appeals for denied claims.
5. Enhances knowledge and skills to keep up to date.	5.1 Attends continuing education activities. 5.2 Keeps abreast and maintains files of current changes in coding requirements from Medicare, Medicaid, and other third-party payers. 5.3 Assists with updating fee schedules and encounter forms with current codes. 5.4 Assists in the research of proper coding techniques.
6. Employs interpersonal expertise to provide good working relationships with patients, employer, employees, and third-party payers.	6.1 Works with employer and employees cooperatively as a team. 6.2 Communicates effectively with patients and third-party payers. 6.3 Executes job assignments with diligence and skill. 6.4 Assists staff with coding and reimbursement problems. 6.5 Assists other employees when needed.

Fig. 1.2 Generic job description for an insurance billing specialist.

GENERIC JOB DESCRIPTION FOR AN ELECTRONIC CLAIMS PROCESSOR

Knowledge, skills, and abilities:
1. Minimum education level consists of certificate from 1-year insurance billing course, associate degree, or equivalent in work experience and continuing education.
2. Knowledge of basic medical terminology, anatomy and physiology, diseases, surgeries, medical specialties, and insurance terminology.
3. Ability to operate computer and printer, as well as photocopy and calculator equipment.
4. Written and oral communication skills including grammar, punctuation, and style.
5. Ability and knowledge to use procedure code books.
6. Ability and knowledge to use diagnostic code books.
7. Knowledge and skill of data entry.
8. Ability to work independently.
9. Certification in electronic claims processing is preferred.

Salary:
Employer would list range of remuneration for the position.

Job responsibilities:	Performance standards:
1. Acts as a link between the medical provider or facility and third-party payers.	1.1 Uses knowledge of medical terminology, anatomy, diseases, surgeries, and medical specialties. 1.2 Understands computer applications and equipment required to convert and transmit patient billing data electronically. 1.3 Consults reference materials as needed. 1.4 Meets accuracy and production requirements.
2. Converts patient billing data into electronically readable formats.	2.1 Inputs data and transmits insurance claims accurately, either directly or through a clearinghouse. 2.2 Answers routine inquiries related to insurance data transmitted to third-party payers. 2.3 Updates and maintains software applications as needed.
3. Uses software that eliminates common claim filing errors, provides clean claims to third-party payers expedites payments, and follows, up on delinquent or denied claims.	3.1 Codes procedures and diagnoses accurately. 3.2 Telephones third-party payers about delinquent claims. 3.3 Traces insurance claims. 3.4 Files appeals for denied claims.
4. Exhibits an understanding of ethical and medicolegal responsibilities related to insurance billing programs and plans.	4.1 Observes policies and procedures related to federal privacy regulations, health records, release of information, retention of records, and statute of limitations for claim submission. 4.2 Meets standards of professional etiquette and ethical conduct. 4.3 Recognizes and reports problems involving fraud, abuse, embezzlement, and forgery to appropriate individuals.
5. Follows employer's policies and procedures.	5.1 Must have punctual work attendance and be dependable.
6. Enhances knowledge and skills to keep up to date.	6.1 Attends continuing education skills activities. 6.2 Obtains current knowledge applicable to transmission of insurance claims. 6.3 Keeps abreast and maintains files of current changes in coding requirements from Medicare, Medicaid, and other third-party payers. Assists in the research of proper coding techniques to maximum reimbursement.
7. Employs interpersonal expertise to provide good working relationships with patients, employer, employees, and third-party payers.	7.1 Works with employer and employees cooperatively as a team. 7.2 Communicates effectively with patients and third-party payers. 7.3 Executes job assignments with diligence and skill. 7.4 Assists staff with coding and reimbursement problems. 7.5 Assists other employees when needed.

Fig. 1.3 Generic job description for an electronic claims processor.

Administrative office duties have gained in importance in the medical billing process. In some health care organizations, an insurance billing specialist may act as an insurance counselor, taking the patient to a private area of the office before being seen by the provider. The insurance counselor will discuss the health care organization's financial policies and review the patient's insurance coverage. The counselor confirms with the insurance company any fees the patient is responsible for and verifies whether any preauthorization, precertification, or second-opinion requirements exist. Insurance counselors help to obtain payment in full when expensive procedures are necessary. Insurance counselors ensure that the health care organization will be paid for services rendered and to develop good communication lines.

Front desk staff are responsible for collecting payment from **self-pay patients**. Self-pay patients are those who do not have any medical insurance and are liable for the entire bill. Front desk staff are also responsible for collecting any copayments or deductible amounts from the patient at each encounter before the patient is treated.

After the patient has been treated, the insurance billing specialist should confirm that documentation of services has been completed by the health care provider. Documentation of services is vital to good patient care and must be done comprehensively and timely for proper reimbursement. A coding specialist may review or assign diagnostic and procedural coding which must be supported in the documentation.

Federal and state insurance programs require the provider of services to submit claims for the patient. Other insurance payers may see claim submission as the patient's obligation, although most health care organizations submit all claims for patients as a courtesy. The insurance billing specialist must submit insurance claims promptly, ideally within 1 to 5 business days, to ensure continuous cash flow. **Cash flow** is the amount of actual money generated and available for use by the health care organization within a given period. Without money coming in, overhead expenses such as salaries, rent, supplies, and insurance cannot be met and an organization will face financial difficulties.

In some organizations the insurance biller may act as a collection manager, who answers routine inquiries related to account balances and insurance submission dates; assists patients in setting up a payment schedule that is within their budget; follows up on delinquent accounts; and traces denied, "adjusted," or unpaid claims (Fig. 1.4).

The **accounts receivables** for a health care organization is the total amount of money owed to them for health care services rendered to patients. Having a large accounts receivables is often a direct result of failure to verify insurance plan benefits, obtain authorization or precertification, or collect fees from patients or inadequate claims filing. The rush to get a claim "out the door" cannot be justified when an organization has thousands or millions of dollars in unpaid or denied claims. Accounts receivables will be low and revenue high if the organization takes the extra time to ensure that the claim is 100% accurate, complete, and verified.

Educational and Training Requirements

A high school diploma or equivalent and previous experience in a health care setting may not always be enough for positions as an insurance billing specialist. Typically a postsecondary certificate or an associate's degree is required to enter the field. Postsecondary certificates and associate's degree programs usually include courses in medical terminology, anatomy and physiology, insurance claims completion, procedural and diagnostic coding, health care reimbursement methods, ethics and medicolegal knowledge, computer skills, and general office skills. Completion of an accredited program for coding certification or an accredited health information technology program is necessary for a job as a coder.

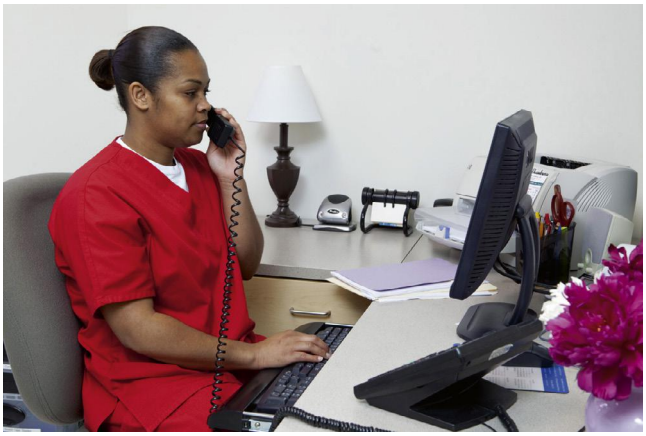

Fig. 1.4 Insurance biller talking to a patient on the telephone about copayment required for an office encounter under the patient's insurance plan.

The curriculum that might be offered in an online certificate program for a medical insurance specialist is shown in Fig. 1.5. A 2-year educational course can result in obtaining an associate's degree. Many accredited programs include an externship, which is a training program with private businesses that gives students brief practical experience in their field of study. It is usually short term but allows the student to gain firsthand insight into the field.

Experience and a moderate to high degree of knowledge of the health insurance business are necessary if the individual's goal is to become a self-employed insurance billing specialist or CAP. In addition to insurance terminology, claims procedures, and coding, a CAP must know commercial insurance payers' requirements as well as Medicare and state Medicaid policies and regulations. Proficiency in running a business, including marketing and sales expertise is also essential.

To reach a professional level of billing or coding expertise, certification is available from many national associations, depending on the type of certification desired. Refer to Chapter 20 for more information on this topic.

Career Advantages

According to the US Bureau of Labor Statistics,[1] employment in the field is expected to grow faster than jobs in other occupations. The demand for health services and related jobs is expected to increase over the next 10 years as the population ages. Jobs are available in every state, ranging from entry level to management positions. Insurance billing specialists can receive a salary of $8000 part-time to $50,000 full-time or more per year, depending on knowledge, experience, duties, responsibilities, locale, and size of the employing institution. Jobs are available with insurance and managed care companies, medical clearinghouses, ambulatory

Medical Billing and Coding Program Curriculum

Curriculum Description:

Students learn the fundamentals of medical billing and coding and are prepared to take the Certified Billing and Coding Specialist (CBCS) exam from the National Healthcareer Association, the Certified Professional Coder (CPC exam) from the American Academy of Professional Coders (AAPC) and the Certified Coding Associate (CCA) exam from the American Health Information Management Association (AHIMA). Program topics include medical terminology, insurance plans, medical ethics, HIPAA, diagnostic and procedural coding, coding compliance and auditing, physician and hospital billing, Medicare, Medicaid and TRICARE. Students receive training on ICD-10-CM/PCS, CPT and HCPCS code assignment.

LESSON GROUPS

Group 1: Introduction to Allied Health • Allied Health Careers	Group 2: Law, Ethics, and Confidentiality in Allied Health • Law in Allied Health • Ethics in Allied Health • Confidentiality in Allied Health
Group 3: Medical Billing and Health Insurance • Reimbursement Methodologies • Comprehensive Health Insurances	Group 4: Medical Office Procedures • Basic Math for Allied Health • Basic Grammar for Allied Health • Professional Communications • Basic Microsoft® Word and Excel
Group 5: Body Systems and Terminology • Introduction to Medical Terminology • Cardiovascular and Hematologic Systems • Respiratory and Endocrine Systems • GI, Urinary, and Reproductive Systems	Group 6: Body Systems and Terminology • Integumentary and Musculoskeletal Systems • Sensory Organs and Nervous System Immune System, HIV, and Cancer
Group 7: Pathology and Pharmacology • Introduction to Pharmacology • Pharmacology • Introduction to Pathology • Pathology	Group 8: Electronic Medical Records • Electronic Health Records and Security • Administrative and Clinical Use of the EHR • Reimbursement and Personal Health Records • Electronic Medical Records Final Exam • Electronic Medical Records Graded Project
Group 9: Basic Medical Coding • Introduction to Coding • Diagnosis Coding with ICD-10-CM • Guidelines for Using ICD-10-CM • Procedure Coding with ICD-10-PCS • Basic Medical Coding Graded Project	Group 10: Intermediate Medical Coding • Introduction to CPT • Evaluation and Management and Anesthesia Coding • Surgical CPT Coding, Part 1 • Surgical CPT Coding, Part 2 • Surgical CPT Coding, Part 3 • Intermediate Medical Coding Graded Project
Group 11: Billing and Coding Professional Certification Exam Review • Anatomy, Terminology and Pathophysiology • CPT Coding • HCPCS Coding and Reimbursement • ICD-10-CM Coding • Post-Exam	

Fig. 1.5 Example of an online medical billing certificate course curriculum. (Reprinted with permission from Ashworth College.)

surgical centers, clinics, hospitals, multispecialty medical groups, and private physicians' practices. Many insurance billing specialists will have the good fortune to advance their careers and move into higher paying positions that come with additional learning, certifications, and experience. These positions may be with consulting firms, instructors at educational facilities, lecturers, or consumer advocates. Other branches of the advanced career field include specialty coding, auditing, compliance, and documentation improvement specialists. These advancement opportunities and certifications will be discussed further in Chapter 20.

Self-Employment or Independent Contracting

After gaining experience, many people establish independently owned and self-operated businesses within their communities as medical insurance billing specialists, coders, claim assistance professionals, collectors, or consultants. However, the responsibilities are greater in this area because such work demands a full-time commitment, a lot of hard work, long hours to obtain clients, and the need to advertise and market the business. The self-employed insurance billing specialist is responsible for everything: advertising, billing, bookkeeping, and other general business tasks.

Flexibility

The nature of medical billing lends itself to flexible hours and flexible job options. The medical insurance billing specialist may want to come in early to transmit electronic claims during off-peak hours or stay late to make collection calls. Many times, medical billing positions have various combinations of work flexibility such as telecommuting, part-time, contract, and work-at-home opportunities. There is an increase in the number of employers who will provide a work-at-home option to highly competent billers and coders who have proven their technical skills and work ethic. In most cases where working from home is allowed, it will be on a hybrid basis, which allows the employees to complete part of their work from home but be required to spend time in the office as well. The availability of work-from-home jobs varies on a case-by-case basis and depends on the employer's policy. Many employers see this type of arrangement as a way to save time, money, and overhead costs while building productivity and increasing job satisfaction.

Disabled Workers

A career as an insurance billing specialist or a collector of delinquent accounts can be rewarding for persons with disabilities. The revenue cycle management responsibilities and other jobs involving telephone communications are an opportunity for someone who is visually impaired because he or she is usually a good listener when properly and specifically trained. Special equipment, such as a Braille keyboard, magnified computer screen, audible scanner, or digital audio recorder, may be necessary to enhance job performance.

Working independently from a home office may appeal to a physically disabled person when there is no need to commute to the health care organization on a daily basis. Accessing information remotely via the computer is a manageable method for success. However, it is important first to gain experience before trying to establish a work-at-home situation.

Qualifications and Attributes

An individual must have a variety of characteristics or qualities to function well as an insurance billing specialist. Strong critical thinking and reading skills with good comprehension are a must. Being a logical and practical thinker, as well as a creative problem solver, is important. Being meticulous and neat makes it easier to get the job done at the workstation. A person with good organizational skills who is conscientious and loyal is always an asset to the employer. Because a large amount of specific data must be obtained, this work requires an individual who is detail oriented. A person with a curious nature will dig deeper into an issue and not be satisfied with an answer unless the "whys" and "whats" are defined. This also helps one to grow while on the job and not become stagnant. Equally important are time management and social skills.

Skills

A person who completes insurance claims must have many skills. One needs the following skills to be proficient Table 1.1:

TABLE 1.1 Skills Application

Skill	Application
Solid foundation and working knowledge of medical terminology, including anatomy, physiology, disease, and treatment terms, as well as the meanings of abbreviations.	Interpretation of patient's chart notes and code manuals. For example, the diagnosis which is documented is ASHD. **ASHD** must be translated to arteriosclerotic hear disease.
Expert use of procedural and diagnostic code books and other related resources.	Code manuals, official coding guidelines, and other reference books are used to assign accurate codes for each case billed.
Precise reading skills.	Differentiate between the technical descriptions of two different but similar procedures. Example: Procedural (CPT) code 43352 Esophagostomy (fistulization of esophagus, external; cervical approach) and Procedural (CPT) code 43020 Esophagotomy (cervical approach, with removal of foreign body). Note that the addition of the letter s to the surgical procedure in the first part of the example changes the entire procedure.
Basic mathematics.	Calculate fees and adjustments on the insurance claim forms and enter them into the patient accounts. It is essential that the figures be accurate
Knowledge of medicolegal rules and regulations of various insurance programs.	Avoid filing of claims considered fraudulent or abusive because of code selection and program policies.
Knowledge of compliance issues.	Federal privacy, security, and transaction rules in addition to fraud, waste, and abuse.

Continued

TABLE 1.1 Skills Application—cont'd

Skill	Application
Basic keyboarding and computer skills.	Good keyboarding and data entry skills and knowledge of computer programs are essential in an industry which utilizes various software programs for management of electronic medical records, management of the revenue cycle, and electronic claims submission
Proficiency in accessing information through the internet.	Obtain federal, state, and commercial insurance regulations and current information as needed through the internet. Sign on as a member of an electronic mailing list where questions may be posted. Find one composed of working coders to obtain answers on how to code complex care, or difficult medical cases.
Knowledge of billing and collection techniques.	Use latest billing and collection ideas to keep cash flow constant and avoid delinquent accounts.
Expertise in the legalities of collection on accounts.	Avoid lawsuits by knowing state and federal collection laws as they apply to medical collection of accounts receivable.
Ability to generate insurance claims with speed and accuracy.	Independent medical claims and billing specialists are often paid according to the amount of paid claims the health care practice is reimbursed. Because they rely on volume for income, the more expeditious they become, the more money they earn. Therefore accuracy in selecting the correct codes and data entry and motivation in completing claims also become marketable skills.
Excellent communication skills	Insurance billing specialists communicate with health car eproviders and other professionals to collect accurate information for billing purposes. The communicate with patients and insurance carriers to collect fees and resolve pending and denied claims. Many specialists also communicate with health care administrative professionals as part of revenue cycle management. Having a pleasant tone and friendly attitude are important skills for an effective communicator. Insurance billing specialists must have empathy when communicating with patients and confidence when working with health care professionals and insurance carriers. In all cases, communications should be clear and concise.

Personal Image

To project a professional image, the insurance billing specialist must be attentive to apparel and grooming (Fig. 1.6). Health care professionals are expected to present themselves in an appropriate and professional manner that portrays an image of confidence and security to the patient. Appearance and perception play a key role in patient service.

When hired, it is important to request the organization's dress-code policy. A **dress code** is a set of guidelines identifying what is appropriate for the employee to wear to work. The insurance billing specialist might be expected to wear scrubs or business attire that is conservative and frequently referred to as *business casual*. Distracting items in appearance or dress, low-cut clothing, exposed midriff, T-shirts, or sheer clothing are typically considered unacceptable. It is absolutely necessary for health care professionals to present neat and clean in the professional setting. Fingernails should be carefully manicured and appropriate to the dress code. Employers may also have guidelines regarding body piercings and tattoos. Keep in mind that fragrances can be offensive or cause allergies to some co-workers and patients; therefore, use good judgment. An example of a dress code policy is shown in (Fig. 1.7).

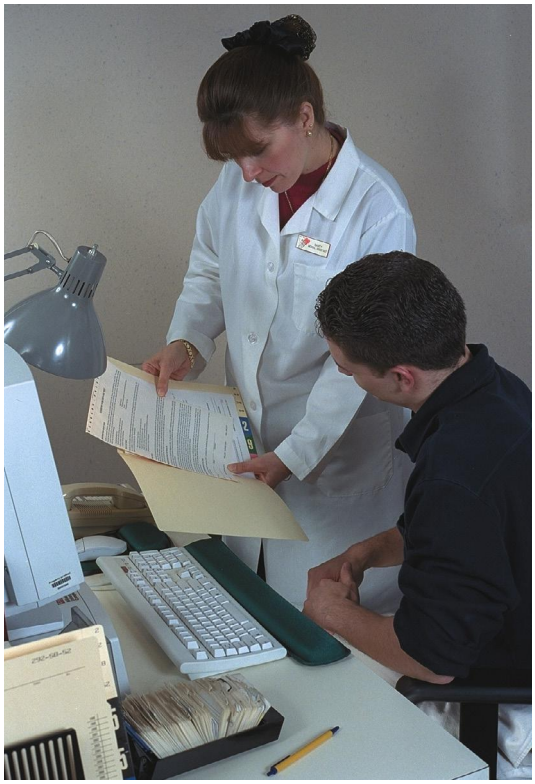

Fig. 1.6 Male and female medical personnel who project a clean, fresh, and professional image.

Behavior

Many aspects make an individual a true professional: getting along with people rates high on the list, as does maintaining confidentiality of patients' health information. An insurance billing specialist depends on many co-workers for information needed to bill claims; therefore it is necessary to be a team player and treat patients and co-workers with courtesy and respect. Consider all co-workers' duties as important because they are part of the team, working together to reach the goal of processing the billing and obtaining maximum reimbursement for the patient and the health care organization. Communicate effectively. Be honest, dependable, and on time. Never take part in office gossip or politics.

1.2 QUICK REVIEW

Question: What is cash flow and why is it important?

XYZ Medical Practice

Dress Code Policy
Insurance Billing Specialist

Introduction:
Appearance and perception play a key role in patient services. Dress, grooming and personal cleanliness standards contribute to the morale of all employees and affect the professional image we present to patients and visitors.

The XYZ Medical Practice's dress code policy is designed to provide our staff with consistent and appropriate guidance as we strive to maintain a professional appearance at all times. The goal is to provide an image of confidence and security to our patients.

Designated Staff: Insurance Billing Specialist

Policy:

- Employees are expected to dress in scrubs or business casual attire. Business casual includes: dress pants, Docker-type pants, khakis, slacks, casual skirts or dresses of appropriate length, shirts with collars, blazers, sports coats, sweaters, golf shirts/polo shirts and blouses.
- Blue jeans are not permitted with the exception of "jean day" to raise money for charity.
- Inappropriate attire includes (but is not limited to): shorts, sweatpants, spandex leggings, wind suits, miniskirts and spaghetti strap tops and sundresses.
- Clothing with offensive or inappropriate designs or stamps are not allowed.
- Clothing should not be too revealing
- Employees must always present a clean and professional appearance. Staff should be well-groomed and wear clean clothing.
- Hair should be clean, combed and neatly trimmed. This includes sideburns, mustaches and beards.
- Due to possible allergies of co-workers and patients, it is requested that staff do not wear fragrances.
- ID badges should be worn in a visible place above the waist at all times.

Dress Code Violations:
The guidelines established in this policy cannot be all-inclusive. Therefore, management will make the final decision as to the appropriateness of work attire as needed.

Office managers are responsible for ensuring appearance is appropriate and are expected to inform staff when they are violating the dress code. Staff in violation are expected to immediately correct the issue. This may include having to leave work to change clothes. Repeated violations or violations that have major repercussions may result in disciplinary action being taken up to and including termination.

Fig. 1.7 Example of a dress code policy for an insurance billing specialist.

MEDICAL ETIQUETTE

Before beginning work as an insurance billing specialist, it is wise to have a basic knowledge of medical **etiquette** as it pertains to the medical profession, the insurance industry, and the medical coder. Medical etiquette has to do with how medical professionals conduct themselves, their behavior. Customs, courtesy, and manners of the medical profession can be expressed in three simple words: *consideration for others.*

In every business that interacts with customers or clients, the focus begins with good customer service. Co-workers and patients should always be acknowledged with a smile, a nod, or a greeting. Patients may arrive for their appointments ill or injured

and suffering from a lot of negativity. If a mistake is made, there is power in an apology given at the first sign of trouble. Attentiveness and a helpful, friendly atmosphere can smooth out the kinks and wrinkles of stressful and negative situations. All people have the need to feel special and they gravitate toward individuals who make them feel that way. All of these personal skills mean good customer service and satisfaction and can lead to professional success for the insurance billing specialist and the health care organization.

Several points about medical etiquette bear mentioning, as follows:

1. Always connect another health care provider who is calling on the telephone to the provider immediately, asking as few questions as possible.
2. Follow the basic rules of etiquette with co-workers while working in the office, such as acknowledging people entering the work area and by saying, "I'll be with you in a moment."
3. Clearly identify yourself when placing or receiving calls.
4. Do not use first names unless permission to do so has been given.
5. Maintain a professional demeanor and a certain amount of formality when interacting with others. Remember to be courteous and always project a professional image.
6. Observe rules of etiquette when sending e-mail messages and placing or receiving cellphone calls.
7. Practice cultural awareness by understanding and respecting the differences of others. Be sensitive to differences in attitudes, values, and perceptions.

Proper etiquette may make the difference between a highly satisfied patient and a disgruntled patient. Proper etiquette lets the patient know that you value them and that your organization is happy to help them.

EXAMPLE 1.1 Electronic Mail Address

Electronic mail (e-mail) address mason@gmail.com means:
Mason individual user (Mason)

@	at
gmail	site (an online service provider)
com	type of site (commercial business)

Electronic Mail Etiquette

Electronic mail (e-mail) is the transmitting, receiving, storing, and forwarding of text, voice messages, attachments, or images by computer from one person to another. Every computer user subscribing to an online service may establish an e-mail address (Example 1.1).

Because this is a more cost-effective and efficient method of sending a message to someone and obtaining a quicker response, insurance billing specialists frequently compose, forward, and respond via e-mail with staff in other locations, with patients, and with insurance billers (Fig. 1.8). It is important to set some standards to follow when communicating via e-mail. The messages sent are a reflection of an individual's professional image.

1. Compose the message in a clear and concise manner using good grammar and proper spelling. Make sure it cannot be misconstrued.
2. Clearly identify the reason for the message in the subject line. If a reply changes the topic, then change the subject line.
3. Do not put confidential information in an e-mail message (e.g., patient-identifiable information).
4. Encrypt (code) all files about patients and e-mail attachments and limit the size of attachments.

Address ➔	To: apcconsulting@gmail.com
Subject Line ➔	Subj: **anesthesia modifiers**
Date ➔	Date: Friday, April 17, 2020
Sender Address ➔	From: brownm@xyz.org
Salutation ➔	Dear Madam or Sir:
Left ➔ Justified Brief Message With Proper Grammar	Question: Is conscious sedation considered anesthesia in relationship to modifier -73 and -74? A speaker at a recent conference said "yes" but another said it had not yet been clarified by CMS. Our fiscal intermediary manual has an example that said modifier -52 would be used in conjunction with a colonoscopy with conscious sedation. What is correct?
Complimentary Closing ➔	Sincerely,
Signature Line ➔	Mary Brown
Title ➔	Insurance Billing Specialist
Location ➔	XYZ Ambulatory Surgery Center
E-mail address ➔	brownm@xyz.org
Confidentiality Statement ➔	IMPORTANT WARNING: This e-mail (and any attachments) is only intended for the use of the person or entity to which it is addressed, and may contain information that is privileged and confidential. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Unauthorized re-disclosure or failure to maintain confidentiality may subject you to federal and state penalties. If you are not the intended recipient, please immediately notify us by return e-mail, and delete this message from your computer.

Fig. 1.8 Electronic mail message sent to an ambulatory surgical center consultant asking a question about the use of modifiers.

5. Recognize that all e-mail is discoverable in legal proceedings, so be careful with content and choice of words.
6. Do not use all capital letters for more than one word.
7. Insert a blank line between paragraphs.
8. Surround URLs (long web addresses) with angle brackets [] to avoid problems occurring at the end of a line because of the word wrap feature.
9. Do not use variable text styles (bold or italic) or text colors.
10. Quote sparingly when automatically quoting the original message in replies. Quotation marks should be inserted to differentiate original and new text.
11. Avoid sending or forwarding junk messages (e.g., welcome messages, congratulation messages, jokes, chain messages).
12. Avoid "**emoticons**," a short sequence of keyboard letters and symbols used to convey emotion, gestures, or expressions (e.g., "smiley" [(:-)]).
13. Avoid "**text speak**," which is the process of shortening words and using abbreviations that do not follow standard grammar, spelling, and punctuation. (e.g. "TY" for "thank you" or "IMO" for "in my opinion".
14. Do not respond immediately to e-mails that result in negative emotions or anger. Put the message aside until the next day and then answer it diplomatically.
15. Do not write anything that is racially or sexually offensive.
16. A short signature at the end of the message should be inserted that includes the sender's name, affiliation, and e-mail and/or URL address.
17. When replying to emails with multiple addresses, make sure to respond only to the desired individual.

1.3 QUICK REVIEW

Question: What are three simple words that can be used to express customs, courtesy, and manners of any medical professional?

PROFESSIONAL ETHICS

Ethics are not laws but standards of conduct generally accepted as moral guides for behavior. Ethics should be relied upon as the insurance billing specialist relates with patients, health care providers, co-workers, the government, and insurance companies. Insurance billing specialists are entrusted with holding patients' medical information in confidence, collecting money for their health care organization, and being a reliable resource for co-workers. To act with ethical behavior means carrying out responsibilities with integrity, decency, honesty, competence, consideration, respect, fairness, trust, and courage.

The earliest written code of ethical principles and conduct for the medical profession originated in Babylonia about 2500 BC and is called the *Code of Hammurabi*. Then, about the fifth century BC, Hippocrates, a Greek physician who is known as the "Father of Medicine," conceived the Oath of Hippocrates.

In 1980 the **American Medical Association (AMA)** adopted a modern code of ethics, called the *Principles of Medical Ethics,* for the benefit of the health professional and to meet the needs of changing times. The Principles of Medical Ethics of the AMA (Box 1.1) guide physicians' standards of conduct for honorable behavior in the practice of medicine.

BOX 1.1 Principles of Medical Ethics of the American Medical Association

Preamble

The medical profession has long subscribed to a body of ethical statements developed primarily for the benefit of the patient.

As a member of the profession, a physician must recognize responsibility to patients first and foremost, as well as to society, to other health professionals, and to self. The following principles adopted by the AMA are not laws, but standards of conduct that define the essentials of honorable behavior for the physician.

I. A physician shall be dedicated to providing competent medical service with compassion and respect for human dignity and rights.
II. A physician shall uphold the standards of professionalism, be honest in all professional interactions, and strive to report physicians deficient in character or competence, or engaging in fraud or deception to appropriate entities.
III. A physician shall respect the law and also recognize a responsibility to seek changes in those requirements which are contrary to the best interests of the patient.
IV. A physician shall respect the rights of patients, of colleagues, and of other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law.
V. A physician shall continue to study, apply, and advance scientific knowledge, maintain a commitment to medical education, make relevant information available to patients, colleagues, and the public; obtain consultation; and use the talents of other health professionals when indicated.
VI. A physician shall, in the provision of appropriate patient care, except in emergencies, be free to choose whom to serve, with whom to associate, and the environment in which to provide medical care.
VII. A physician shall recognize a responsibility to participate in activities contributing to the improvement of the community and the betterment of public health.
VIII. A physician shall, while caring for a patient, regard responsibility to the patient as paramount.
IX. A physician shall support access to medical care for all people.

Revised June 2001. Permission granted to reproduce by the American Medical Association.

It is the insurance billing specialist's responsibility to inform administration or their immediate supervisor if unethical or possibly illegal billing or coding practices are taking place. Illegal activities are subject to penalties, fines, and/or imprisonment and can result in loss of morale, reputation, and the goodwill of the community.

The following are principles of ethics for the insurance billing specialist:

- Never make critical remarks about a health care organization or provider to a patient or anyone else. Maintain dignity; never belittle patients.
- Notify a supervisor if it is discovered that a patient may have questionable issues of care, conduct, or treatment with the health care organization or another provider.

Maintain a dignified, courteous relationship with all persons in the office—patients, staff, and health care providers—as well as with insurance adjusters, pharmaceutical representatives, and others who come into or telephone the office (Fig. 1.9).

It is *illegal* to report incorrect information to government-funded programs, such as Medicare, Medicaid, and TRICARE.

Fig. 1.9 A mental health professional working in a dignified manner with patients. (Copyright © iStock/SDI Productions.)

Federal legislation has been passed on fraud and abuse issues that relate to federal health care programs. However, private insurance payers operate under different laws and it is *unethical but may not be illegal, depending on state laws,* to report incorrect information to private insurance payers. Incorrect information may damage the individual and the integrity of the database, allow reimbursement for services that should be paid by the patient, or deny payment that should be made by the insurance company.

Most professional organizations for insurance billing specialists or coders have established a code of ethics for their members to follow. A sample code of ethics is shown in Fig. 1.10.

In the final analysis, most ethical issues can be reduced to right and wrong with the focus being the moral dictum to do no harm.

American Health Information Management Association

STANDARDS OF ETHICAL CODING

Coding professionals should:

1. Apply accurate, complete and consistent coding practices that yield quality data.
2. Gather and report all data required for internal and external reporting, in accordance with applicable requirements and data set definitions.
3. Assign and report, in any format, only the codes and data that are clearly and consistently supported by health record documentation in accordance with applicable code set and abstraction conventions, and requirements.
4. Query and/or consult as needed with the provider for clarification and additional documentation prior to final code assignment in accordance with acceptable healthcare industry practices.
5. Refuse to participate in, support, or change reported data and/or narrative titles, billing data, clinical documentation practices, or any coding related activities intended to skew or misrepresent data and their meaning that do not comply with requirements.
6. Facilitate, advocate, and collaborate with healthcare professionals in the pursuit of accurate, complete and reliable coded data and in situations that support ethical coding practices.
7. Advance coding knowledge and practice through continuing education, including but not limited to meeting continuing education requirements.
8. Maintain the confidentiality of protected health information in accordance with the Code of Ethics.
9. Refuse to participate in the development of coding and coding related technology that is not designed in accordance with requirements.
10. Demonstrate behavior that reflects integrity, shows a commitment to ethical and legal coding practices, and fosters trust in professional activities.
11. Refuse to participate in and/or conceal unethical coding, data abstraction, query practices, or any inappropriate activities related to coding and address any perceived unethical coding related practices.

Revised and approved by AHIMA's House of Delegates December 12, 2016

Fig. 1.10 American Health Information Management Association (AHIMA) Standards of Ethical Coding, revised and adopted by AHIMA House of Delegates, 2016. (Copyright © 2018 American Health Information Management Association. All rights reserved. Permission granted to reproduce.)

1.4 QUICK REVIEW

Question: What moral dictum can an insurance billing specialist rely upon when faced with an ethical issue?

SCOPE OF PRACTICE AND LIABILITY

Most health care professions have a well-defined scope of practice that easily draws a boundary on things that professionals can do and things they are not supposed to do. The field of medical billing and coding does not have such a well-defined scope of practice. Instead, professionals in this field are guided by job descriptions, codes of ethics, coding policies, internal compliance policies, insurance carrier policies, and health care regulations. Regardless of whether they are involved in facility or professional billing, they must be aware of their own liability.

Employer Liability

As mentioned, insurance billing specialists can be either self-employed or employed by physicians, clinics, hospitals, or ancillary service providers. The health care organization that employs the insurance billing specialist is legally responsible for its own conduct and any actions of its employees performed within the context of their employment. This is referred to as *vicarious liability,* also known as **respondeat superior**, which literally means "let the master answer." However, this does not mean that an employee cannot be sued or brought to trial. Actions of the insurance biller may have a definite legal ramification on the employer, depending on the situation. For example, if an employee knowingly submits a fraudulent Medicare or Medicaid claim at the direction of the employer and subsequently the business is audited, both the employer and employee can be brought into litigation by the state or federal government. An insurance biller always should check with their employer to determine whether they are included in the medical **professional liability insurance** policy, otherwise known as malpractice insurance. If not included, he or she could be sued as an individual. It is the health care organization's responsibility to make certain all staff members are protected.

Employee Liability

Billers and coders can be held personally responsible under the law for billing errors and have been listed as defendants in billing-fraud lawsuits. An insurance billing specialist who knowingly submits a false claim or allows such a claim to be submitted can be liable for a civil violation. If they conceal information or fail to disclose it to obtain payment, they can be held liable. Even if they did not prepare the false claim, the individual who mails or electronically files the claim may also be implicated in mail or wire fraud. Fraud will be covered in greater detail in Chapter 3.

If any staff member within a health care organization, or any provider of services, asks the insurance biller to do something that is the least bit questionable, such as writing off patient balances for certain patients automatically, it is recommended that the biller contact their supervisor and make sure they have a legal document or signed waiver of liability relieving them of the responsibility for such actions. When such problems are noted, it is the insurance billing specialist's responsibility to correct it and to document their actions in writing.

Independent Contractor Liability

Independent contractors are those who may have decided to establish their own self-operated business as a medical insurance billing specialist, coder, or consultant. These individuals perform services for health care organizations under contract and are not covered under the organization's professional liability insurance.

Independent contractors should purchase **errors and omissions insurance**, which provides protection against loss of money caused by failure through error or unintentional omission on the part of the individual or service involved in any aspect of preparation or submission of an insurance claim. Independent contractors can often purchase errors and omission insurance though professional organizations they may belong to.

Claims Assistant Professional Liability

An individual who works as a CAP acts as an informal representative of patients, helping them to obtain insurance reimbursement. A CAP reviews and analyzes existing or potential policies, renders advice, and offers counseling, recommendations, and information. A CAP may not interpret insurance policies or act as an attorney. The legal ability of a CAP to represent a policyholder is limited. When a claim cannot be resolved after a denied claim has been appealed to the insurance company, the CAP must be careful in rendering an opinion or advising clients that they have a right to pursue legal action. State regulations should always be checked to see whether there is a scope of practice. In some states, a CAP could be acting outside the scope of the law by giving advice to clients on legal issues, even if licensed as an attorney but not practicing law full time. If the client wishes to take legal action, it is their responsibility to find a competent attorney specializing in contract law and insurance. In some states, giving an insured client advice on purchase or discontinuance of insurance policies is construed as being an insurance agent.

A number of states require CAPs to be licensed, depending on the services rendered to clients. CAPs who perform only the clerical function of filing health insurance claims do not have to be licensed. Check with the state's department of insurance and insurance commissioner to determine whether licensing is required.

1.5 QUICK REVIEW

Question: Can billers and coders be held personally responsible under the law for billing errors?

FUTURE CHALLENGES

An insurance billing specialist must remember that they are expected to manage a health care organization's financial affairs accurately; otherwise, they will not be considered qualified for

this position. Subsequent chapters contain valuable information to help develop the knowledge and skills necessary to help achieve this goal. Insurance billing specialists will be expected to do the following:

- Know billing regulations for each insurance program in which the health care organization is a participant.
- Know the aspects of compliance rules and regulations.
- State various insurance rules about treatment and referral of patients.
- Become proficient in computer skills and use of various medical software packages.
- Learn electronic billing software and the variances of each payer.
- Develop diagnostic and procedural coding expertise.
- Know how to interpret insurance carrier's remittance advice summary reports, explanation of benefit documents, or both.
- Attain bookkeeping skills necessary to post, interpret, and manage patient accounts.
- Keep current and stay up to date by reading the latest health care industry association publications, participating in e-mail listserv discussions, joining a professional organization for networking, and attending seminars on billing and coding.
- Insurance billing specialists should train to also become familiar with other aspects of the health care organization.
- Discover opportunities for career advancement.
- Strive toward becoming certified as an insurance billing specialist and/or coder and, once certified, seek continuing education credits to become recertified.

Becoming an insurance billing specialist is the first step into an exciting career that has endless opportunities. Chapter 20 will provide information into some of the more advanced roles that the billing specialist can work toward and the professional organizations that offer certification.

DISCUSSION POINT

Describe why you are training to become an insurance billing specialist?

PROCEDURE 1.1 Analyze Professional Ethics and Medical Etiquette

Objectives: To analyze how professional ethics and medical etiquette are essential qualities for insurance billing specialists

Directions:

1. Review and identify the difference between professional ethics and medical etiquette.
2. With a classmate, make a list of ways the insurance billing specialist could observe rules of medical etiquette when discussing claims with patients.
3. With a classmate, make a list of ways the insurance billing specialist could practice professional ethics when discussing claims with patients.
4. With a classmate, role-play a situation in which the insurance billing specialist is being challenged by a frustrated and angry patient who has an outstanding bill with the health care organization.

KEY POINTS

This is a brief chapter review, or summary, of the key issues presented.

1. The medical insurance billing specialist's primary goal is to help patients obtain maximum insurance plan benefits for the services they received while ensuring the cash flow of their organization through revenue cycle management.
2. The health care industry is one of the most heavily regulated industries in the U.S. which contributes to the complexities of medical billing.
3. The person who does facility or professional billing has become a proficient specialist known by a number of job titles, such as insurance billing specialist or reimbursement specialist.
4. Insurance claims must be promptly submitted to ensure continuous cash flow for a health care organization. If not, overhead expenses cannot be met and the organization will face financial difficulties.
5. Because of the increased technical knowledge that a biller must have, education and training must be more comprehensive and skills must be developed in coding and claims completion. When proficiency is reached, a person can work for a health care organization or may possibly set up their own billing service. In this career, jobs can be rewarding for persons with disabilities.
6. Individuals who do billing and complete insurance claims must have many skills, such as knowledge of medical terminology and abbreviations, expert use of procedural and diagnostic code books, precise reading skills, ability to perform basic mathematic calculations, knowledge of medicolegal rules and regulations of various insurance programs, ability to understand and apply compliance issues, basic computer skills (keyboarding and software applications), proficiency in accessing information via the internet, ability to carry out billing and collection techniques, expertise in the legalities of collection on accounts, and ability to generate insurance claims expediently and accurately.
7. Becoming a professional is a gradual process and one must project an appropriate image and develop themselves as a courteous and respectful team player.
8. Etiquette in a medical setting must be adhered to routinely. The insurance billing specialist must display customs, courteousness, and manners that always show consideration of others.
9. A health care organization that employs an insurance billing specialist is legally responsible for any actions its employees perform within the context of their employment. This is referred to as vicarious liability, also known as *respondeat superior.*
10. Remember, ignorance of the law is not a protection for anyone working in a health care organization, so one must stay up to date and well informed on state and federal statutes.

STUDENT ASSIGNMENT

Read the Introduction in the *Workbook,* which explains how you will be working as an insurance billing specialist during this course.

- Study Chapter 1.
- Complete all exercises in the *Workbook* to reinforce the theory learned in this chapter.
- Turn to the Glossary at the end of this book for a further understanding of the key terms and key abbreviations used in this chapter.

2

Privacy, Security, and HIPAA

Cheryl Fassett

OBJECTIVES

After reading this chapter, you should be able to:

1. Name the two provisions of the Health Insurance Portability and Accountability Act (HIPAA) that relate most to health care.
2. Explain the difference between *Title I: Health Insurance Reform* and *Title II: Administrative Simplification.*
3. Define and discuss HIPAA roles, relationships, and key terms, including HIPAA in the practice setting.
4. Describe the Privacy Rule under HIPAA.
5. Define and discuss protected health information (PHI).
6. Illustrate the difference between privileged and nonprivileged information.
7. Identify the difference between disclosure and use of PHI and discuss exceptions to HIPAA.
8. State the guidelines for HIPAA privacy compliance.
9. Explain patient rights under HIPAA.
10. Explain responsibilities of the health care organization to protect patient rights under HIPAA.
11. Define the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).
12. Discuss the Security Rule and how it relates to coding and billing.
13. List the three major categories of security safeguards under HIPAA.
14. Explain the purpose of the HIPAA Omnibus Rule.
15. List consequences of noncompliance with HIPAA and the HITECH Act.
16. Discuss how HIPAA affects all areas of the health care office, including the organization and staff responsibilities in protecting patient rights.

KEY TERMS

administrative safeguards
American Recovery and Reinvestment Act
authorization
authorization form
breach
business associate
clearinghouse
confidential communication
confidentiality
consent
covered entity
designated record sets
disclosure
electronic protected health information
employer identification number
health care organization
health care provider
The Health Information Technology for Economic and Clinical Health Act
Health Insurance Portability and Accountability Act
HIPAA Omnibus Rule
incidental use and disclosure
individually identifiable health information
Minimum Necessary Rule
mitigation
National Provider Identifier
nonprivileged information
Notice of Privacy Practices
Office of Inspector General
Patient Protection and Affordable Care Act of 2010
physical safeguards
portability
preexisting condition
privacy
privacy officer, privacy official
privacy rule
privileged information
protected health information
psychotherapy notes
security officer
Security Rule
state preemption
technical safeguards
transaction
use

KEY ABBREVIATIONS

ARRA	FBI	IIHI	PHI
CMS	FTP	NPI	PO
DHHS	HHS	NPP	P&P
EIN	HIPAA	OCR	PPACA
ePHI	HITECH	OIG	TPO

INSIGHTS FROM THE FIELD

Cindy B.: Certified Professional Coder (CPC), Certified Professional Medical Auditor (CPMA)

I started as an Emergency Department Services coder in 2006 and am a Clinical Coding Supervisor. I oversee medical coding for various services provided by the hospital and nursing facilities. I also manage physician educators who balance reimbursement and compliance.

I think being inquisitive is the most valuable skill. Never be afraid to question anything! The hardest part of joining this field is accepting that many of the concepts are not just black and white. Having a solid understanding of the basics and the foundation of coding allows each of us to justify our coding decisions, and defend ourselves in audits. I try to stress this to any of my newer coders; they will continue to build their skills, but there is no shortcut to learning the basics.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY

One of the most important pieces of legislation to have an impact on health care organizations, health care workers, and patients is the **Health Insurance Portability and Accountability Act (HIPAA)** of 1996. The Act is made up of five titles. Among these five titles, there are two provisions that relate most to health care: *Title I: Health Insurance Reform* and *Title II: Administrative Simplification*. The goals of HIPAA were as follows:

- Assure health insurance portability
- Enforce standards for health information
- Reduce health care fraud and abuse
- Guarantee security and privacy of an individual's health information

The Department of Health and Human Services (**DHHS** or **HHS**) is the US government's principal agency for protecting the health of all Americans and providing essential human services. HIPAA legislation required the DHHS to establish national standards and identifiers for electronic transactions as well as to implement privacy and security standards.

The Office of E-Health Standards and Services, a division of the Centers for Medicare and Medicaid Services (**CMS**), enforces the insurance portability and transaction and code set requirements for Medicare and Medicaid programs.

The Office for Civil Rights (**OCR**) enforces privacy and security rules. It is a part of DHHS. The OCR protects our rights under nondiscrimination laws and HIPAA privacy laws. It investigates violations of these rights as well as patient safety issues.

The projected long-term benefits of HIPAA legislation include the following:

- Lowered administrative costs
- Increased accuracy of data
- Increased patient and customer satisfaction
- Reduced revenue cycle time, and
- Improved revenue cycle management

Title I: Health Insurance Reform

The primary purpose of HIPAA *Title I: Health Insurance Reform* is to provide insurance **portability**, or continuous insurance coverage for workers and their dependents when they change or lose jobs. Under this provision, an employee has the right to maintain health care benefits under a group health plan when leaving a job. The former employee has the option to continue their group health plan benefits; however, he or she is responsible for the *total* cost of the benefit.

Previously, when an employee left or lost a job and changed insurance coverage, coverage was limited for preexisting conditions. A **preexisting condition** is an illness or injury that began prior to when the insurance went into effect. HIPAA now limits the use of preexisting condition exclusions. It also prohibits discrimination for past or present medical conditions, and guarantees certain individuals the right to purchase new health insurance coverage after losing a job. HIPAA also allows renewal of health insurance coverage regardless of an individual's health condition.

It is also important to understand what HIPAA *Title I* does *not* do. HIPAA does not force employers to offer health insurance. It also does not regulate how much insurance companies can charge for premiums.

Title II: Administrative Simplification

HIPAA *Title II: Administrative Simplification* focuses on reducing administrative costs and burdens for health care organizations. Standardizing electronic transmissions of billing and payment information reduces the number of forms and methods used in processing claims. This reduces the effort needed to process paper or nonstandard electronic claims.

Additional provisions are meant to ensure the privacy and security of an individual's health data. *Title II* also focuses on reducing fraud, waste, and abuse in health care by increasing both the funding to combat fraud and abuse and the penalties associated with fraudulent activities.

There are four main parts of HIPAA *Title II* that directly pertain to health care organizations:

- Standard Transactions and Code Sets
- Unique Identifiers
- Privacy and Confidentiality
- Security of Health Transactions

2.1 QUICK REVIEW

Question: What were the four main goals of HIPAA legislation?

TRANSACTION AND CODE SETS

HIPAA requires the use of standard code sets to represent health care concepts and procedures. This reduces the number of forms and standardizes the method used to process claims. It allows providers, facilities, and other health care organizations to code and submit claims in the exact same format for every payer, thereby reducing cost and effort. This was not the case before HIPAA when every health plan could require a different format and additional nonstandard information. It made the billing process time consuming and difficult.

The standard code sets required in HIPAA include the following:

- International Classification of Disease, Tenth Revision, Clinical Modification (ICD-10-CM, Volumes I and II) for diagnosis coding
- International Classification of Disease, Tenth Revision, Procedure Coding System (ICD-10-PCS) for hospital and facility procedure coding
- Current Procedural Terminology (CPT) for professional health care procedure coding
- Healthcare Common Procedure Coding System (HCPCS) for nonphysician services and supply coding
- Current Dental Terminology (CDT) for dental procedure coding

CMS refers to a ***transaction*** as the electronic exchange of information between two parties to carry out financial or administrative activities related to health care. These data exchanges include information that completes the insurance claim process and are discussed later in the text. These transactions are typically done in an electronic format, though paper claims processing is still an option.

HIPAA electronic transaction standards require all covered entities to use the same format. All payers are then required to communicate payment, denial, and pended claims in the same format as well. These transaction and code set standards create a common language among health care providers and payers, thereby increasing the efficiency of the claims process. Types of transactions that transmit sensitive data are as follows:

- Claims and encounter information
- Payment and remittance advice
- Claims status
- Eligibility
- Enrollment and disenrollment
- Referrals and authorizations
- Coordination of benefits, and
- Premium payments

2.2 QUICK REVIEW

Question: What are the standard code sets required by HIPAA?

NATIONAL IDENTIFIERS

HIPAA *Title II* also mandates the creation of a National Identifier system. This assigns unique identifiers to every health care organization, employer, health plan, and patient. The purpose of the identifiers is to further standardize electronic transmissions of claim data.

While the first two types of identifiers were implemented after HIPAA became law, the health plan identifiers were not officially mandated until the **Patient Protection and Affordable Care Act of 2010 (PPACA)**. Patient identifiers are still in the discussion phase. Proponents claim the use of unique patient identifiers will increase patient safety and help with the digitizing of health care data. Those who are against it raise concerns over privacy.

The Internal Revenue Service assigns **employer identifier numbers (EINs)** to employers. Also known as tax identification numbers (TINs), they identify an employer in all electronic transactions from payroll to health plan enrollment.

National Provider Identifiers (NPIs) are unique identifiers assigned to every health care organization, employer, health plan, and patient. These are used to submit and process health care claims. If a billing specialist submits a claim for a provider in a health care organization, both the provider's NPI and the health care organization's NPI must appear on the claim.

2.3 QUICK REVIEW

Question: What is an NPI?

THE PRIVACY RULE: CONFIDENTIALITY AND PROTECTED HEALTH INFORMATION

Federal and state regulations, professional standards, and ethics all address patient privacy. In the past, health care organizations simply locked health records in file cabinets and often refused to share patient health information. Now, under HIPAA, patients have specific rights regarding how their health information is used and disclosed. Knowledge of and attention to the rights of patients are important to being compliant in a health care organization.

Health care staff are entrusted with private information that can identify a person such as name, date of birth, and social security number. They also have access to private health information and are expected to recognize when certain health information can be used or disclosed. Health care organizations and their employees can be held accountable for using or disclosing patient health information inappropriately. Following privacy and security procedures prevents the misuse of health information.

Computers are essential to health care organizations. Confidential health data is now sent across networks and e-mailed over the internet. Sometimes few safeguards are taken to protect data and prevent information from being lost or intercepted by hackers. With the implementation of standardized electronic transactions of health care information, the use of technology poses new risks for privacy and security. HIPAA addresses these concerns.

Regulations now closely govern how the industry handles its electronic activities. The HIPAA **Privacy Rule** establishes national standards to protect individuals' health records and other personal health information. It applies to all covered entities that conduct health care transactions electronically.

The HIPAA Privacy Rule has three main objectives:

1. to protect patient information from being used and disclosed inappropriately
2. to give patients greater control over sharing of information, and
3. to increase patient access to information.

Privacy, Confidentiality, Use, and Disclosure

Privacy is the condition of being secluded from the presence or view of others. **Confidentiality** is using discretion in keeping information secret. An employee must have strong moral principles and integrity and must be committed to protecting the privacy and rights of the health care organization's patients.

Health care organizations and their staff use and disclose health information on a regular basis. **Use** means the sharing, application, utilization, examination, or analysis of health information within the organization. For example, when a patient's billing record is accessed to review the claim submission history, the individual's health information is in use. Records are also shared between providers in the course of patient care; information is released to health plans to process claims.

Disclosure means the release, transfer, provision of access to, or divulging information to people or entities outside the health care organization. An example of a disclosure is a scheduler giving information about a patient when setting them up for a procedure to the health care facility's outpatient surgery center. See Table 2.1 for examples of uses and disclosures of PHI.

TABLE 2.1 *Title II: Administrative Simplification*: Uses and Disclosures of Protected Health Information

Permitted Disclosures (No Authorization Required)	**What It Means for a Health Care Organization**
Disclose PHI to patient	A health care provider may discuss the patient's own medical condition with him or her. **Doing so does not require signed authorization from the patient.**
Disclose PHI for treatment	Treatment includes speaking with the patient, ordering tests, writing prescriptions, coordinating their care, and consulting with another health care provider about the patient. **"Treatment" does not require signed authorization from the patient.**
Disclose PHI for payment	Payment includes obtaining the patient's eligibility or benefits coverage information from the insurance payer, obtaining preapproval for treatment, and billing and managing the claims process. **"Payment" does not require signed authorization from the patient.**
Disclose PHI for health care operations	Do not confuse this with performing surgery. The term *health care operations* refers to the business activities in which the organization participates. Examples include case management, certification, accreditation, medical reviews, and audits to detect fraud and abuse. **"Operations" do not require signed authorization from the patient.**
Disclose PHI for public purposes	PHI may be disclosed for public health purposes, such as reporting a communicable disease, injury, child abuse, domestic violence, judicial and administrative proceedings, law enforcement, coroner or medical examiner, or research purposes, if PHI is "de-identified." This is not an all-inclusive list, but **these examples do not require signed authorization from the patient.**
Disclose PHI for workers' compensation	A billing specialist may disclose PHI as authorized by the laws relating to workers' compensation. Such disclosures to programs that provide benefits for work-related injuries or illness **do not require signed authorization from the patient.**
Disclosures That Require Patient's Opportunity to Agree or Object	**What It Means for a Health Care Organization**
Disclose PHI to persons involved with the patient	An organization must provide patients with an opportunity to object to sharing PHI with family, friends, or others involved with their care. The health care provider can use professional judgment when disclosing PHI to a person involved with the patient's care when the patient is not present. **This requires the patient to have the opportunity to agree or object.**
Disclosures (Authorization Required)	**What It Means for a Health Care Organization**
Disclose psychotherapy notes	Psychotherapy notes may not be disclosed without authorization except for use by the notes' originator (therapist) for treatment. **Signed authorization *is* required.**
Disclose PHI to a child's school for permission to participate in sports	A health care organization may not disclose a child's PHI to a school to permit the student's participation in a sports activity. **Signed authorization *is* required.**
Disclose PHI to employer	A health care organization may not disclose PHI to a patient's employer unless the information is necessary to comply with OSHA, MSHA, or other state laws. **With certain exceptions, signed authorization *is* required.**
Disclose PHI to insurer	A health care organization may not disclose PHI to an insurer for underwriting or eligibility without authorization from the patient (for example, if the patient is trying to obtain a life insurance policy). **Signed authorization *is* required.**
Disclose PHI for fundraising or marketing	If the health care organization does fundraising or marketing activities, it may not disclose PHI without prior authorization from the patient. **Signed authorization *is* required.**

MSHA, Mine Safety and Health Administration; *OSHA*, Occupational Safety and Health Administration; *PHI*, protected health information.

Covered Entities

Under HIPAA, a **covered entity** is any health care provider, health care organization, health plan, or clearinghouse that transmits health information in electronic form for any number of transactions. The covered entity may be (1) a health plan carrier, such as Medicare or Blue Cross/Blue Shield; (2) a health care clearinghouse through which claims are submitted; or (3) a health care provider, such as a primary care physician, hospital, or laboratory.

A **health care provider** is a person trained and licensed to provide care to a patient or a place that is licensed to give health care. A provider may work in a hospital, skilled nursing facility, inpatient/outpatient rehabilitation facility, home health agency, hospice program, physician, diagnostic department, outpatient physical or occupational therapy department, or rural clinic or with a home dialysis supplier. A provider may be a physician, physician's assistant, nurse practitioner, social worker, chiropractor, dentist, and so on.

HIPAA's definition of a **health care organization** extends to entities that provide health care services to a patient. In addition to provider groups, this includes hospitals, ambulance service providers, clinics, nursing homes, pharmacies, and others.

A health care **clearinghouse** is an organization that acts as a go-between for a health care organization and the entity to which health care information is transmitted. It is an independent organization that receives insurance claims from the health care organization, performs software edits, and reformats data as needed into proper format. It then sends the claims electronically to various third-party payers.

HIPAA requires the designation of a **privacy officer or privacy official (PO)**. A PO is an individual who is tasked with helping the health care organization remain in compliance by setting policies and procedures (**P&P**) and by training and managing the staff regarding HIPAA and patient rights. The PO is usually the contact person for questions and complaints. This advisory role in larger organizations may be filled by an attorney or other professional with extensive compliance experience. In smaller health care organizations such as individual or small groups of health care providers, the PO may be an employee who consults with an attorney as needed.

A **security officer** protects the computer and networking systems within the health care organization and implements protocols such as password assignment, backup procedures, firewalls, virus protection, and contingency planning for emergencies. Larger organizations such as hospital systems may have an entire information technology (IT) department working in coordination with the security officer. A smaller organization may assign the role of security officer to the practice manager who may be supported by an outside IT consultant.

Business Associates

A **business associate** is a person or entity that performs certain functions or activities using health care information on behalf of a covered entity. It is considered an extension of the health care organization and is held to the same standards under HIPAA. A business associate performs or assists in the performance of a function or activity involving the use or disclosure of health information. These functions include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. For example, if a health care provider contracts with an outside billing company to manage its claims and accounts receivable, the billing company would be a business associate of the provider (the covered entity).

Covered entities should have a business associate agreement in place with all entities that work with them. The agreement needs to specifically outline how the business associate complies with HIPAA legislation. If a health care provider either transmits directly or uses a business associate, such as a billing company or clearinghouse, to send information electronically for any of the transactions listed, all parties are a covered entity and must comply with HIPAA.

Protected Health Information

Protected health information (PHI) is any information that identifies an individual and describes their health status, age, sex, ethnicity, or other demographic characteristics, whether that information is stored or transmitted electronically. It refers to any part of the patient's health information that is transmitted by electronic media, maintained or stored in electronic form, or in any other form or medium. See Example 2.1 for examples of PHI. Traditionally, privacy focused on protecting paper health records that held patient's health information, such as laboratory results and radiology reports. HIPAA Privacy Rule expands these protections to apply to PHI. The individual's health information is protected regardless of the type of medium in which it is maintained. This includes paper, the organization's computerized medical billing system, spoken words, and x-ray films.

EXAMPLE 2.1 Examples of Protected Health Information

- Name
- Address
- Telephone Number
- Social Security Number
- Health Record Number
- Driver's License Number
- Account Number
- Health Plan ID Number
- Date of Birth
- Dates of admission/discharge
- Date of Death
- Email Address
- Biometric Identifiers (i.e. fingerprint)
- Photographic Images

Individually Identifiable Health Information

Individually identifiable health information (IIHI) is any part of an individual's health information, including demographic information, collected from the individual by a covered entity. This information relates to the individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care. IIHI data identify the individual or establish a reasonable basis to believe that the information can be used to identify the individual. For example, if a health care provider is talking to an insurance representative, they will likely give information such as the patient's date of birth and last name. These pieces of information would make it reasonably easy to identify the patient. Conversely, if a staff

member in a health care organization is talking to a pharmaceutical representative about a drug assistance program that covers a new pill for heartburn and says that the organization has a patient living in a particular town who is indigent and has stomach problems, the staff member is not divulging information that would identify the patient.

Other requirements relating to uses and disclosures of PHI focus on information that does not identify an individual or leaves no reasonable basis to believe that the information can be used to identify an individual. This de-identified information is no longer considered to be individually identifiable health information (IIHI). The regulations give specific directions on how to ensure that all pieces of necessary information are removed to fit the definition. De-identified information is not subject to the privacy regulations because it does not specifically identify an individual.

Privileged and Nonprivileged Information

When working with health records, all health care staff members are responsible for maintaining the confidentiality of patients' health information. The purpose of the Privacy Rule is to ensure that patients who receive medical treatment can control the manner in which specific information is used and to whom it is disclosed.

Confidential communication is a privileged communication that may be disclosed only with the patient's permission. Everything a health care worker sees, hears, or reads about patients remains confidential and does not leave the office. Never talk about patients or data contained in health records where others may overhear. Some employers require employees to sign a confidentiality agreement (Fig. 2.1). Such agreements should be updated periodically to address issues raised by the use of new technologies.

EMPLOYEE CONFIDENTIALITY STATEMENT

As an employee of ABC Clinic, Inc. (employer), having been trained as an insurance billing specialist with employee responsibilities and authorization to access personal medical and health information, and as a condition of my employment, I agree to the following:

A. I recognize that I am responsible for complying with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 policies regarding confidentiality of patients' information, which, if I violate, may lead to immediate dismissal from employment and, depending on state laws, criminal prosecution.

B. I will treat all information received during the course of my employment, which relates to the patients, as confidential and privileged information.

C. I will not access patient information unless I must obtain the information to perform my job duties.

D. I will not disclose information regarding my employer's patients to any person or entity, other than that necessary to perform my job duties, and as permitted under the employer's HIPAA policies.

E. I will not access any of my employer's computer systems that currently exist or may exist in the future using a password other than my own.

F. I will safeguard my computer password and will not show it in public.

G. I will not allow anyone, including other employees, to use my password to access computer files.

H. I will log off of the computer immediately after I finish using it.

I. I will not use e-mail to transmit patient information unless instructed to do so by my employer's HIPAA privacy officer.

J. I will not take patient information from my employer's premises in hard copy or electronic form without permission from my employer's HIPAA privacy officer.

K. Upon termination of my employment, I agree to continue to maintain the confidentiality of any information learned while an employee and agree to relinquish office keys, access cards, or any other device that provides access to the provider or its information.

Mary Doe
Signature

September 14, 20XX
Date

Mary Doe
Print name

Brenda Shield
Witness

Fig. 2.1 An example of an employee confidentiality agreement that may be used by an employer when hiring an insurance billing specialist.

Privileged information is related to the treatment and progress of the patient. The patient must sign an authorization to release this information or selected facts from the health record. Some states have passed laws allowing certain test results (e.g, the presence of the human immunodeficiency virus [HIV] or alcohol or substance abuse) and other information to be maintained separate from the patient's health record. Some states require a special authorization form be used to release this information.

Example 2.2 lists some of the privileged communications that a health care organization might use that fall under HIPAA compliance regulations.

EXAMPLE 2.2 Privileged Communications in a Health Care Organization

- Intake forms
- Laboratory work requests
- Provider–patient conversations
- Conversations that refer to patients by name
- Provider dictation tapes
- Telephone conversations with patients
- Encounter sheets
- Provider notes
- Prescriptions
- Insurance claim forms
- X-ray films
- E-mail messages

Nonprivileged information consists of ordinary facts unrelated to treatment of the patient, including the patient's name, city of residence, and dates of admission or discharge. This information must be protected from unauthorized disclosure under the privacy section of HIPAA. The patient's authorization is not necessary for the purposes of treatment, payment, or health care operations, unless the record is in a specialty health care facility such as an alcohol treatment center or a special service unit of a general hospital such as a psychiatric unit. Professional judgment is required. The information is disclosed on a legitimate need-to-know basis. For example, an attending physician may require complete access to the health record because the information may have some effect on the treatment of the patient, but an x-ray technician would not necessarily need to know everything in the record.

! COMPLIANCE ALERT

Confidentiality Statement

Most information in patients' health records and the health care organization's financial records is considered confidential and sensitive. Employees who have access to such computer data should have integrity and be well chosen because they have a high degree of responsibility and accountability. It is wise to have those handling sensitive computer documents sign an annual confidentiality statement (see Fig. 2.1). This way the statement can be updated when an individual's responsibilities increase or decrease. The statement should contain the following:

- Written or oral disclosure of information pertaining to patients is prohibited.
- Disclosure of information without consent of the patient results in serious penalty or immediate dismissal.

Designated Record Set

HIPAA gives an individual the right to access their health information in a designated record set maintained by each covered entity and its business associates. **Designated record sets** include health records, billing and claims records, and health plan enrollment records. A patient is not guaranteed access to information that is not part of a designated record set. Some examples of information that a covered entity is not required to release to a patient are peer reviews, patient safety control records, and business planning records. Other information not included in a designated record set are appointment schedules, requests for diagnostic testing, and birth and death records.

Psychotherapy Notes

Psychotherapy notes have special protection under HIPAA. Disclosure of a patient's mental health records requires specific patient permission. This means that when an insurance payer requests the health records to review the claim, a patient authorization is required.

In general, **psychotherapy notes** are defined as the information that is the recorded (in any manner) documentation and/or analysis of conversation with the patient. This information should be kept separate from the medical section of the patient health record to be distinguished as psychotherapy notes. For example, Jane Doe tells her psychologist the details of her childhood trauma. The documented conversation specific to her trauma (e.g, what occurred and how she felt) is considered the psychotherapy notes and cannot be released without Jane Doe's specific permission.

Certain clinical data are excluded from the definition of psychotherapy notes. When an individual is using the services of a mental health professional, not all information gathered and recorded in the health record of the mental health provider is considered part of the psychotherapy notes. The law lists the following specific items that are excluded from such notes:

- Medication prescription and monitoring
- Counseling session start and stop times
- Modalities and frequencies of treatment furnished
- Results of clinical tests
- Any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date

It is also important to understand that patients do not have the right to obtain a copy of psychotherapy notes under HIPAA. However, the treating mental health provider can decide when a patient may obtain access to this health information. State law must always be considered. Some states allow patients access to their psychotherapy notes. In these cases, state law would take precedence over HIPAA as a result of the state preemption allowance as described later in this chapter.

Consent and Authorizations

HIPAA imposes requirements to protect not only disclosure of PHI outside of the organization but also internal uses of health information. PHI may not be used or disclosed without permission from the patient or someone authorized to act on behalf of the patient. However, the rule does allow the use or disclosure of PHI if it is specifically for the purposes of treatment, payment, or health care operations (**TPO**).

Consent is the verbal or written agreement that gives approval to some action, situation, or statement. With regards to HIPAA, a consent is a document that gives health care organizations

permission to use or disclose PHI for TPO. Although many health care organizations obtain signed consents from their patients, the Privacy Rule does not require a covered entity to obtain consent for routine uses and disclosures. See Fig. 2.2 for an example of a consent for release of information for TPO.

Treatment includes coordination or management of health care between providers or referral of a patient to another provider. PHI can also be disclosed to obtain reimbursement or payment for services. Other health care operations include performance reviews, audits, and training programs.

In contrast to a consent, the HIPAA Privacy Rule requires a signed **authorization** for any uses and disclosures that are not routine and are not otherwise allowed by the Privacy Rule. Authorization is an individual's formal, written permission to use or disclose their personally identifiable health information for purposes other than TPO. The authorization must specify the information to be disclosed and the purpose of the disclosure. It must specify who is disclosing the information and who is receiving it. For example, if a patient changes primary care providers, they will need to sign an authorization to have their

COLLEGE CLINIC
4567 Broad Avenue
Woodland Hills, XY 12345-0001
Phone: 555/486-9002
Fax: 555/487-8976

CONSENT TO THE USE AND DISCLOSURE OF HEALTH INFORMATION

I understand that this organization originates and maintains health records which describe my health history, symptoms, examination, test results, diagnoses, treatment, and any plans for future care or treatment. I understand that this information is used to:

- plan my care and treatment.
- communicate among health professionals who contribute to my care.
- apply my diagnosis and services, procedures, and surgical information to my bill.
- verify services billed by third-party payers.
- assess quality of care and review the competence of health care professionals in routine health care operations.

I further understand that:

- a complete description of information uses and disclosures is included in a *Notice of Information Practices* which has been provided to me.
- I have a right to review the notice prior to signing this consent.
- the organization reserves the right to change their notice and practices.
- any revised notice will be mailed to the address I have provided prior to implementation.
- I have the right to object to the use of my health information for directory purposes.
- I have the right to request restrictions as to how my health information may be used or disclosed to carry out treatment, payment, or health care operations.
- the organization is not required to agree to the restrictions requested.
- I may revoke this consent in writing, except to the extent that the organization has already taken action in reliance thereon.

☐ I request the following restrictions to the use or disclosure of my health information.

_____

_____ Date

_____ Notice Effective Date

_____ Signature of Patient or Legal Representative

_____ Witness

_____ Signature

_____ Title

Date _____

__ Accepted __ Rejected

Fig. 2.2 An example of a consent form used to disclose and use health information for treatment, payment, or health care operations (TPO). This is not required under Health Insurance Portability and Accountability Act (HIPAA), some health care organizations use it. (From Fordney, M. T., & French, L. (2003). *Medical insurance billing and coding: A worktext.* Philadelphia: Elsevier.)

health records sent to the new provider. Health care organizations must be careful when obtaining authorizations for marketing, research, and **psychotherapy notes**. The **authorization form** must state if a health care organization receives remuneration for specific marketing or research activities. See Fig. 2.3 for an example of an authorization for release of information.

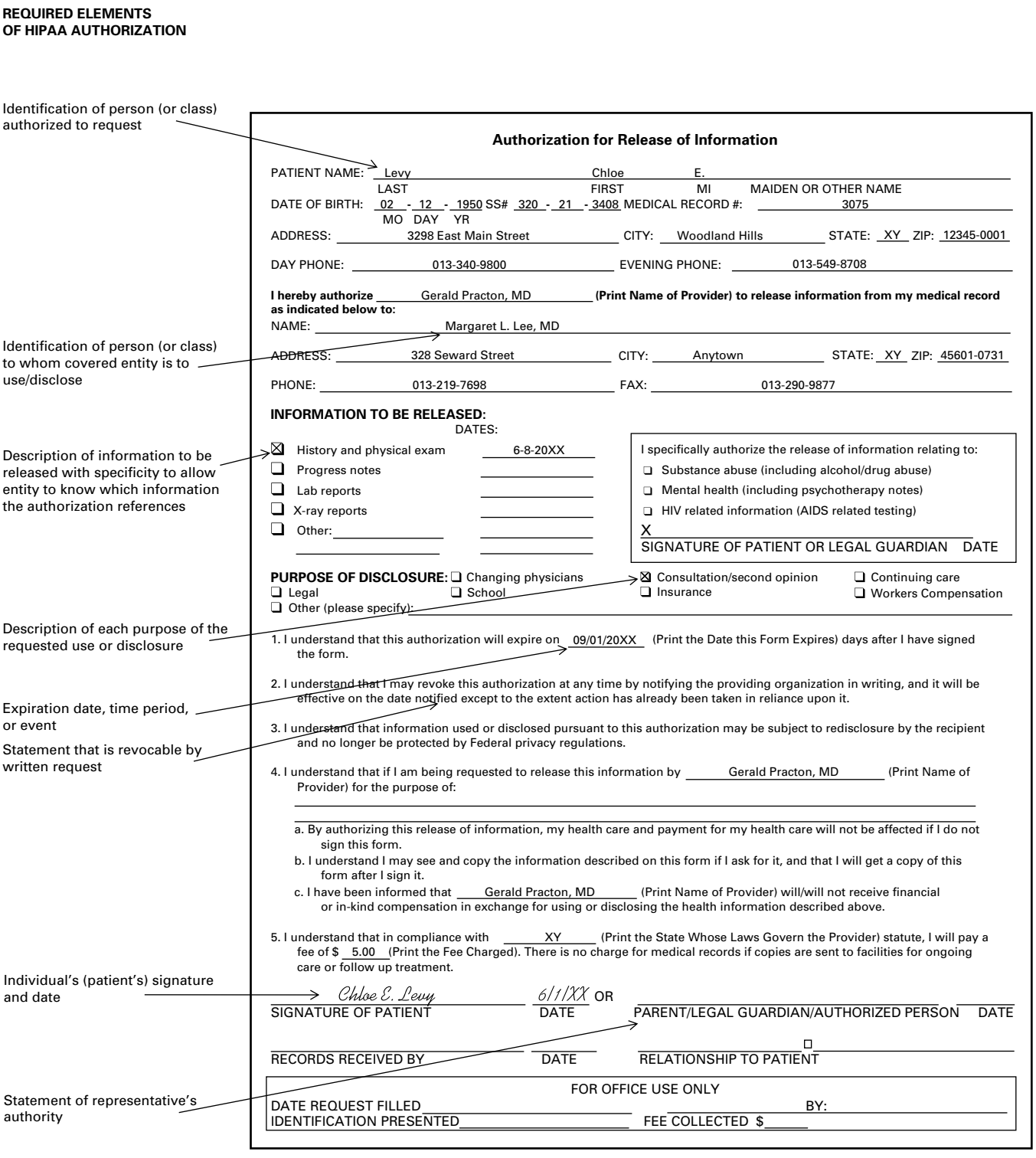

Fig. 2.3 Completed authorization for release of information form for a patient who is seeking a consult or second opinion. The required elements for Health Insurance Portability and Accountability Act (HIPAA) authorization are indicated. Note: This form is used on a one-time basis for reasons other than treatment, payment, or health care operations (TPO). When the patient arrives at the new provider's office, a consent for TPO form will need to be signed. (From *Federal Register* 64[212]: Appendix to Subpart E of Part 164: Model Authorization Form, November 3, 1999.)

Verification of Identity and Authority

Before any disclosure, a health care worker must verify the identity of persons requesting PHI if they are unknown to them. They may request identifying information, such as date of birth, Social Security number, or even a code word stored in the health care organization's medical billing system that is unique to each patient. Public officials may present badges, credentials, official letterheads, and other legal documents of authority for identification purposes. Patients and patient representatives should be prepared to show a valid picture ID such as a driver's license.

Health care workers must also verify that the requestor has the right to receive the PHI and identify the need for the PHI. Exercising professional judgment fulfills the verification requirements for most disclosures because the health care worker is acting on "good faith" in believing the identity of the individual requesting PHI. It is good practice when making any disclosure to note the authority of the person receiving the PHI and how this was determined. This shows due diligence with respect to HIPAA.

Any conflicts among various permissions the organization may have on file for a given patient must be resolved before information can be released. For example, if a covered entity has agreed to a patient's request to limit how much of the PHI is sent to a consulting physician for treatment but then receives the patient's authorization to disclose the entire health record to that provider, this would be a conflict. In general, the more restrictive permission would take precedence. Privacy regulations allow resolving conflicting permissions either by obtaining a new permission from the patient or by communicating orally or in writing with the patient to determine the patient's preference. Be sure to document any form of communication in writing.

Minimum Necessary Rule

Another way that HIPAA restricts access to PHI within an organization is through the **Minimum Necessary Rule**. This requires that the amount of PHI accessed be limited to the minimum amount necessary for a medical staff member to do their job. It should only be shared on a need-to-know basis. Minimum Necessary determinations for *uses of PHI* must be made within each organization and reasonable efforts must be made to limit access to only the minimum amount of information needed by staff members.

In smaller offices, employees may have multiple job functions. If a medical assistant helps with the patient examination, documents vital signs, and then collects the patient's copayment at the reception area, the assistant will likely access both clinical and billing records. Similarly, a coding specialist will need access to the patient's entire health record to code an encounter. However, the receptionist for a health care organization will most likely not need to see the entire record to schedule an appointment for a patient.

Larger organizations may have specific restrictions regarding who should have access to different types of PHI, because staff members tend to have more targeted job roles. Simple procedure and policy (P&P) about appropriate access to PHI may be sufficient to satisfy the Minimum Necessary requirement.

The Minimum Necessary Rule applies to business associates as well. If a provider is referring a patient to a prosthetic manufacturer, he would be violating the minimum necessary rule if he sent the patient's entire health record. The prosthetic manufacturer does not need to know everything the patient was treated for in the past.

Minimum Necessary determinations for *disclosures of PHI* are distinguished by two categories within the Privacy Rule:

1. For disclosures made on a routine and recurring basis, policies and procedures, or standard protocols, may be implemented for what will be disclosed. These disclosures would be common in the organization. Examples may include disclosures for workers' compensation claims or school physical forms.
2. For other disclosures that would be considered nonroutine, criteria for determining the Minimum Necessary amount of PHI should be established and each request for disclosure should be reviewed on an individual basis. A staff member such as the privacy officer (PO) will likely be assigned to determine this situation when the need arises.

Incidental Uses and Disclosures

Reasonable safeguards must be in place to demonstrate that a health care organization is following the HIPAA Privacy Rule. The safeguards are measurable solutions based on accepted standards that are implemented and periodically monitored to show that the office is in compliance. Reasonable efforts must be made to limit the use or disclosure of PHI. For example, if the front desk receptionist closes the privacy glass between their desk and the waiting area when making a call to a patient, this is a reasonable safeguard to prevent others in the waiting room from overhearing.

Incidental uses and disclosures are permissible under HIPAA only when reasonable safeguards or precautions have been implemented to prevent misuse or inappropriate disclosure of PHI. When incidental uses and disclosures result from failure to apply reasonable safeguards or adhere to the minimum necessary standard, the Privacy Rule has been violated. If the receptionist closes the privacy glass before having a confidential conversation but is still overheard by an individual in the waiting room, this would be incidental. They have applied a reasonable safeguard to prevent their conversation from being overheard.

The OCR has addressed what is permissible with regard to incidental disclosures. Examples follow.

- A provider may discuss a patient's condition or plan of care in the patient's treatment area or hospital room.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter or with a provider or the patient by telephone.

- A patient's name may be called out in the reception room; however, some offices prefer to use first names and not call out last names.

State Preemption

HIPAA's federal privacy regulations apply unless the state laws are more stringent regarding privacy, a situation referred to as **state preemption**. A state law is considered to be more stringent if it does the following:

- Gives an individual greater access to their health information
- Prohibits disclosure that would be allowed under HIPAA
- Narrows the duration of an authorization to release information

State preemption is a complex technical issue. It refers to instances when state law takes precedence over federal law. The PO determines when the need for preemption arises.

For example, under HIPAA, a covered entity is required to provide an individual access to their health records in a timely manner (30 or 60 days with a possible extension) from the time they are requested. Under New York State law, a provider must permit visual inspection within 10 days and furnish a copy within a reasonable time. In this situation, New York State law would preempt HIPAA and a provider will have to provide visual inspection within a shorter time frame.

Exceptions to HIPAA

There are exceptions to HIPAA. Confidentiality between the provider and patient is automatically waived in the following situations:

- When the patient is a member of a managed care organization (MCO) and the health care organization has signed a contract with the MCO, the MCO has a right to access the health records of their patients, and, for utilization management purposes, the MCO has a right to audit the patient's financial records.
- When patients have certain communicable diseases that are highly contagious, state health agencies require providers to report them. This is true even if the patient does not want the information reported.
- When a medical device breaks or malfunctions, the Food and Drug Administration (FDA) requires health care organizations to report information that will allow it to be advised of the break or malfunction.
- When a patient is a suspect in a criminal investigation or to assist in locating a missing person, material witness, or suspect, police have the right to request certain information.
- When the patient's records are subpoenaed or there is a search warrant, the courts have the right to order health care organizations to release patient information.
- When there is a suspicious death or suspected crime victim, health care organizations must report cases to proper law enforcement authorities.
- When the provider examines a patient at the request of a third party who is paying the bill, the payer has the right to request information. An example of this would be a workers' compensation carrier requesting an independent medical examination on a patient.
- When state law requires the release of information to police that is for the good of society, proper authorities are allowed to access certain information. Examples of this would be cases of child abuse, elder abuse, domestic violence, or gunshot wounds.

2.4 QUICK REVIEW
Question: What are the objectives of the HIPAA Privacy Rule?

2.5 QUICK REVIEW
Question: What is a covered entity?

2.6 QUICK REVIEW
Question: What is PHI? Give some examples.

2.7 QUICK REVIEW
Question: What is TPO?

2.8 QUICK REVIEW
Question: What is the Minimum Necessary Rule?

PATIENT'S RIGHTS UNDER HIPAA

All patients have a right to privacy. It is important never to discuss patient information other than with the provider, an insurance company, or an individual who has been authorized by the patient. Under HIPAA, patients are granted the following six federal rights that allow them to be informed about PHI and to control how their PHI is used and disclosed (Box 2.1).

BOX 2.1 Health Insurance Portability and Accountability Act Help

In summary, patients have the right to the following:

- Be informed of the organization's privacy practices by receiving a Notice of Privacy Practices (NPP)
- Have their information kept confidential and secure
- Obtain a copy of their health records
- Request to have their health records amended
- Request special considerations in communication
- Restrict unauthorized access to their confidential health information

Patients cannot prevent their confidential health information from being used for treatment, payment, or routine health care operations (TPO), nor may they force amendments to their health record. As a billing specialist become acclimated to their organization's policies and procedures regarding the handling of protected health information (PHI), they will be better able to recognize that their position plays an important part in Health Insurance Portability and Accountability Act compliance.

Required Notice of Privacy Practices

Under HIPAA, a patient has the right to see a health care organization's Notice of Privacy Practices. A **Notice of Privacy Practices (NPP)** is a document that is usually given to the patient at the first

encounter with a provider or at enrollment with a health plan. The staff must make a reasonable best effort to obtain a signature from the patient acknowledging receipt, and also have it signed by a witness. If the patient cannot or will not sign, this should be documented in the patient's record. The NPP must be posted at every service site and be available in paper form for those who request it. A health care organization's website must have the NPP placed on the site and must deliver a copy electronically on request.

A NPP must be in plain language and contain the following information:

- How the covered entity may use or disclose PHI
- The patient's rights regarding PHI and how to file a complaint
- The covered entity's legal duties including how it is required by law to maintain the privacy of the PHI
- Who the patient may contact for further information about the covered entity's privacy policies

To better understand the requirements of the NPP, refer to Procedure 2.1 at the end of the chapter.

! COMPLIANCE ALERT

Health care organizations are expected to handle requests made by patients to exercise their rights. Health care workers must know their organization's process for dealing with each specific request. Understanding HIPAA and the organization's policy manual will guide the worker to follow the appropriate protocol.

Billing specialists should be familiar with the general forms used within the health care organization. Be aware of the following:

- **Written acknowledgment.** After providing the patient with the Notice of Privacy Practices (NPP), a "good faith" effort must be made to obtain written acknowledgment from the patient receiving the document. If the patient refuses to sign or is unable to sign, this must be documented in the patient record.
- **Authorization forms.** Use and disclosure of protected health information (PHI) is permissible for treatment, payment, or routine health care operations (TPO) because the NPP describes how PHI is used for these purposes. The health care organization is required to obtain signed authorization to use or disclose health information for situations beyond TPO. This functions as protection for the organization. Health care staff must learn about the particular authorization forms used in their office.

Restrictions on Certain Uses and Disclosures of Protected Health Information

Patients have the right to request restrictions on certain uses and disclosures of their PHI. For example, a patient who had a successfully treated sexually transmitted infection many years ago can request that, whenever possible, this material not be disclosed. A health care organization is not required to agree to these requests but must have a process to review the requests, accept and review any appeal, and give a sound reason for not agreeing to a request. Restrictions must be documented and followed. Patients also have the right to revoke any authorization they have given for use and disclosure.

Confidential Communications

Patients have the right to request confidential communications by alternative means or at an alternative location. For example, patients may request a provider call them at work rather than at their home. Patients do not need to explain the reason for the request. The health care office must have a process in place both to evaluate requests and appeals and to respond to the patient. Patients may be required by the office to make their requests in writing. A written document protects the health care organization's compliance endeavors.

Access to Protected Health Information

Patients have the right to access and obtain a copy of their health record. Privacy regulations allow the health care organization to require that the patient make the request for access in writing. Generally, a request must be acted on within 30 days. If the covered entity is unable to respond to the request within 30 days, a one-time 30-day extension may be permitted. If an extension is taken, the health care organization must notify the patient within the initial 30-day period and provide the date that the information will be available.

A health care organization may charge a reasonable, cost-based fee for copies of PHI. This may include only the costs for supplies and labor for copying, postage when mailed, and preparing a summary of the PHI if the patient has agreed to this instead of complete access. If a patient requests an electronic copy of their information or requests that it be transmitted to another person, the covered entity generally must produce it in the form requested if readily producible.

Under HIPAA Privacy Rule, patients do not have the right to access the following:

- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, legal proceedings
- Information exempted from disclosure under the Clinical Laboratory Improvements Act (CLIA) (CLIA will be discussed in Chapter 3)

The office may deny patient access for the previously mentioned reasons without giving the patient the right to review the denial. If the health care provider denies access because the patient would be a danger to themselves or someone else as a result of accessing the confidential health information, the patient has the right to have the denial reviewed by another licensed professional who did not participate in the initial denial decision.

Amendment of Protected Health Information

Patients have the right to request that their PHI be amended. As with other requests, the health care organization may require the request to be in writing. There must be a process to accept and review both the request and any appeal in a timely fashion. The request may be denied for the following circumstances:

- The provider who is being requested to change the PHI is not the creator of the information. For example, a health care provider cannot amend a record sent by a referring provider.
- The PHI is believed to be accurate and complete as it stands in the health care organization's health records.

- The information is not required to be accessible to the patient such as a psychotherapy note.

Generally, the health care organization must respond to a patient's request for amendment within 60 days. If a request is denied, the patient must be informed in writing of the reason for the denial. The patient must also be given the opportunity to file a statement of disagreement.

Accounting of Disclosure of Protected Health Information

Patients have the right to receive an accounting of PHI disclosures. Health care organizations should maintain a log of all disclosures of PHI, either on paper or within the organization's computer system. The process for providing an accounting should be outlined in the health care organization's policy manual. Patients may request an accounting or tracking of disclosures of their confidential information and are granted the right to receive this accounting once a year without charge. Items to be documented must include the following:

- Date of disclosure
- Name of the entity or person who received the PHI, including their address, if known
- Brief description of the PHI disclosed
- Brief statement of the purpose of the disclosure

Disclosures made for TPO, facility directories, and some national security and law enforcement agencies are not required to be recorded.

Facility directories are listings of patients within the facility. Under HIPAA, facilities such as hospitals and nursing homes must be careful about releasing information about the patients in their care. Patient directories may list a patient's name, general condition, and location in the hospital. A patient must be given the opportunity to opt out of the directory. Information may only be released to visitors who ask for a patient by name. Clergy may be given directory information without having to ask for the patient by name.

Information pertaining to infectious disease outbreaks may be released to public health officials. Law enforcement may be given information pertaining to the whereabouts of a fugitive, as well as in cases of suspected abuse or violence. Media must be directed to the facility spokesperson. Public figures such as elected officials and celebrities must be given the same privacy standards as other patients.

Box 2.2 reviews some guidelines for maintaining patient confidentiality.

2.9 QUICK REVIEW

Question: True or False?

_____A reasonable effort should be made to obtain a signed acknowledgment after a patient is given an NPP.

_____A patient cannot revoke their authorization to release PHI.

_____A patient has the right to obtain a copy of their psychotherapy notes in their entirety.

_____A patient has the right to request a provider change information in their health record.

BOX 2.2 Do's and Don'ts of Confidentiality

Don't: Discuss a patient with acquaintances, yours or the patient's.

Don't: Leave patients' records or appointment books exposed on your desk.

Don't: Leave a computer screen with patient information visible, even for a moment, if another patient may see the data.

Do: Make sure the person making a telephone inquiry is who they say they are. Use one of the following methods of verification:

- Ask for one or more of the following items: patient's full name, home address, date of birth, Social Security number, mother's maiden name, dates of service.
- Ask for a callback number and compare it with the number on file.
- Ask the patient to fax a sheet with their signature on it so that you can compare it with the one on file.
- Some health care facilities may assign a code word or number such as a middle name or date that is easy for patients to remember. If a patient does not know the code word, then ask for personal identifying information as mentioned.

Do: Obtain proper authorization from the patient to release information to another person.

Do: Use care when leaving messages for patients on answering machines or with another person. Leave your name, the office name, and the return telephone number. Never attempt to interpret a report or provide information about the outcome of laboratory or other diagnostic tests to the patient. Let the provider handle it.

Do: Properly dispose of notes, papers, and memos by using a shredding device.

Do: Be careful when using the copying machine, because it is easy to forget to remove the original insurance claim or health record from the document glass.

Do: Use common sense and follow the guidelines mentioned in this chapter to help you maintain your professional credibility and integrity.

Do: Access only the minimum amount of privileged information necessary to complete your job.

Don't: Use PHI (including names and addresses) for marketing purposes without the specific authorization of the patient without the specific authorization of the patient. Sending appointment reminders and general news updates about a health care organization and the services it provides is not considered marketing and does not require patient authorization.

THE SECURITY RULE: ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGAURDS

The **Security Rule** comprises regulations related to the security of **electronic protected health information (ePHI)**. This refers to any PHI that is produced, saved, transferred, or received in an electronic form. The Security Rule provides regulations related to electronic transactions and code sets, privacy, and enforcement. The Security Rule addresses only ePHI, but the concept of preserving PHI that will become ePHI makes attention to security for the entire organization important. The P&P required by the Security Rule must be maintained for 6 years after they are no longer in use. The Security Rule is divided into three main sections: administrative safeguards, technical safeguards, and physical safeguards. These safeguards reasonably protect PHI from any use or disclosure that violates HIPAA, whether intentional or unintentional (Box 2.3).

BOX 2.3 Examples of Safeguards

Administrative	Technical	Physical
Verifying the identity of an individual picking up health records	Create username and password required to access patient records from computer	Locked, fireproof filing cabinets for storing paper records
Apply sanctions against workforce members who fail to comply with security policies and procedures	Establish procedures to obtain necessary ePHI during an emergency	Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan
Perform regular records review of information system activity, such as audit logs, access reports, and security incident tracking reports	Implement procedures that terminate an electronic session after a predetermined time of inactivity	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users
Identify a security official who will be responsible for the development of policies and procedures	Implement a mechanism to encrypt and decrypt ePHI	Implement policies and procedures to limit physical access to electronic information systems by identifying authorized individuals by title and/or job function

ePHI, Electronic protected health information.

Administrative Safeguards

Administrative safeguards prevent unauthorized use or disclosure of ePHI through information management controls. Policy and procedures to manage this include the selection, development, implementation, and maintenance of security measures to protect ePHI. These measures guard data integrity, confidentiality, and availability and include the following:

- Information access controls, such as passwords, authorize each employee's physical access to ePHI. These restrict access to records in accordance with the employee's responsibility in the health care organization. For example, usually the health information management (HIM) clerk who has authorization to retrieve health records will not have access to billing records. Each user should have a unique username and an unshared, undisclosed password to log in to any computer with access to PHI. Identifying each unique user allows an organization to audit access and ensure proper access controls are implemented. Passwords for all users should be changed on a regular basis and should never be common names or words.
- Internal audits review who has had access to PHI to ensure that there is no intentional or accidental inappropriate access. This applies to both the medical billing systems as well as the paper records.
- Risk analysis and management is a process that assesses the privacy and security risks of various safeguards and the cost in losses if those safeguards are not in place. Each organization must evaluate its vulnerabilities and the associated risks and decide how to lessen those risks. Reasonable safeguards must be implemented to protect against known risks.
- Termination procedures should be formally documented in the P&P manual and include terminating an employee's access to PHI. Other procedures include changing office security pass codes, deleting user access to computer systems, deleting terminated employees' e-mail accounts, and collecting any access cards or keys.

Technical Safeguards

Technical safeguards are security controls that are put in place to protect and track access to information on computers within the health care organization. These include the following:

- Access controls through limitations created for each staff member based on job category. For example, a receptionist, administrative medical assistant, clinical medical assistant, bookkeeper, or insurance billing specialist will have different levels of access depending on their assigned tasks.
- Audit controls keep track of logins to the computer system, administrative activity, and changes to data. This includes changing passwords, deleting user accounts, and creating new user accounts.
- Automatic logoffs prevent unauthorized users from accessing a computer when it is left unattended. The computer system or software program should automatically log off after a predetermined period of inactivity.

Physical Safeguards

Physical safeguards also prevent unauthorized access to PHI. These physical measures and P&P protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards as well as unauthorized intrusion by a hacker or employee who should not have access. Appropriate and reasonable physical safeguards should include the following:

- Media and equipment controls are documented in the P&P manual regarding management of the PHI. Typical safeguard policies include how the office handles the retention, removal, and disposal of paper records as well as recycling computers and destroying obsolete data drives or software programs containing PHI.
- Physical access controls limit unauthorized access to areas in which equipment and medical charts are stored. Locks on doors are the most common type of control.
- Secure workstation locations minimize the possibility of unauthorized viewing of PHI. This includes ensuring

that password-protected screen savers are in use on computers when unattended and that desk drawers are locked.

! COMPLIANCE ALERT

Organizations and their employees can take a number of preventive measures to maintain computer security.

1. Obtain a software program that stores files in coded form.
2. Never leave electronic storage devices unguarded on desks or anywhere else in sight.
3. Use a privacy filter over the computer monitor so that data may be read only when the user is directly in front of the computer.
4. Log off the computer terminal before leaving a workstation.
5. Read the manuals for the equipment, especially the sections titled "Security Controls," and follow all directions.
6. Store confidential data on external media rather than only on the computer's hard drive. External media should be stored in a locked, secure location, preferably one that is fireproof and away from magnetic fields.
7. Make sure the computer system has a firewall and proper antivirus/antispyware software installed. Hackers can also access digital copiers, laser printers, fax machines, and other electronic equipment with internal memories.
8. Send only an account number when e-mailing a colleague with specific questions. Never send the patient's name or other identifying information over unsecured e-mail.
9. Develop passwords for each user and access codes to protect the data. A password is a combination of letters, numbers, or symbols that an individual is assigned to access the system. Passwords should be changed at regular intervals and never written down. A good password is composed of more than eight characters and is case sensitive. *Case sensitive* means that the password must be entered exactly as stored using upper- or lowercase characters. Delete obsolete passwords from the system. Change any passwords known by an employee who is fired or resigns. Individuals with their own passwords allow the employer to distinguish work done by each employee. If errors or problems occur, focus may then be directed toward correcting the individual user.

A strong password:

- Is at least eight characters long.
- Does not contain the username, real name, or company name.
- Does not contain a complete word.
- Is significantly different from a previous password.
- Contains characters from these four categories: uppercase, lowercase, numbers, symbols. For example: Iluv2pla2BA4$

2.10 QUICK REVIEW

Question: Give an example of each type of safeguard: administrative, technical, and physical

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

The **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** was a provision of the **American Recovery and Reinvestment Act (ARRA)** of 2009. ARRA contained incentives for adopting health care IT that are designed to speed up the adoption of electronic health record systems for many health care organizations. The HITECH Act updated and enhanced the privacy and security responsibilities of covered entities that were established under HIPAA. The HITECH Act brought significant compliance changes to three specific areas:

1. Business associates
2. Notification of breach
3. Civil penalties for noncompliance with the provisions of HIPAA

Business Associates

Under HIPAA, the covered entity is responsible and liable for all activities related to their **business associates**. If a covered entity becomes aware of a breach involving a business associate, the covered entity is expected to terminate the contract if the breach was not corrected. The HITECH Act also brought greater responsibility to the business associate. It required all business associates to comply with the HIPAA Security Rule in the same manner that a covered entity would. Business associates are expected to implement physical and technical safeguards as outlined in the Security Rule. They are expected to conduct a risk analysis, to develop and implement related policies and procedures, and to comply with written documentation and workforce training requirements. The business associate is now subject to the application of civil and criminal penalties, just as a covered entity is.

Notification of Breach

The HITECH Act defines a **breach** as the unauthorized acquisition, access, use, or disclosure of PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.

Mitigation means to "alleviate the severity" or "make mild." In reference to HIPAA, the covered entity has a duty to take appropriate steps in response to a breach of confidential communication. Breaches are considered to be HIPAA violations and may lead to substantial fines. If a breach is discovered, the health care organization is required to mitigate, to the extent possible, any harmful effects of the breach. For example, if a billing specialist learns that they have sent health records by fax to an incorrect party, steps should be taken to have the recipient destroy the PHI. Mitigation procedures also apply to activities of the health care organization's business associates. Being proactive and responsible by mitigating reduces the potential for a more disastrous outcome from the breach or violation.

Under the HITECH Act, if a breach were to occur, the HITECH Act requires a covered entity to notify the affected party directly within 60 days. Any breach is presumed reportable unless the covered entity or business associated can demonstrate that there is a low probability that the information has been compromised.

Breach notification is not required when any of the following occur:

1. The breach was unintentional access or use by someone who acquired the PHI in good faith through the normal scope of their job. For example, if a billing specialist receives and opens an e-mail from a nurse, and then notifies the nurse of

the misdirected e-mail and deletes it, a breach notification is not required.
2. There is a good faith belief that the unauthorized person could not have retained the PHI. For example, if a laptop is lost and recovered and analysis shows that information on the laptop had not been accessed or altered, a breach notification is not required.
3. A health care organization may be asked by law enforcement to delay breach notification if such notification would impede an investigation.

If an organization has used an appropriate method to encrypt and destroy files, it is relieved of the breach notification rule as it applies to that PHI.

Breach notification must be sent in writing via first class mail to each individual affected. If the patient is deceased, the next of kin must be notified. If an address is unknown, an effort must be made to reach the individual through other means. If the breach affects 500 or more individuals, the notice must also be provided to local media outlets such as newspaper and television news.

DHHS must also be notified within 60 days of the breach for breaches affecting 500 or more people. For smaller breaches, DHHS can be notified annually or within 60 days of the end of the year the breach was discovered. A list of covered entities that have had breaches is maintained by DHHS. Organizations on this list must submit logs of breaches to the DHHS on an ongoing annual basis.

HIPAA Omnibus Rule

The final **HIPAA Omnibus Rule** is an update to the 1996 HIPAA law and 2009 HITECH Act that modified both privacy and security rules for covered entities and their business associates. The new rule, effective March 26, 2013, did the following:

- enhanced patients' privacy rights and protections, especially regarding genetic information
- strengthened the OCR's ability to enforce the HIPAA privacy and security protections in the face of the expanded use of electronic health records
- held business associates who receive PHI and their subcontractors to the same standards of covered entities
- clarified when breaches of unsecured health information must be reported to DHHS
- increased the restrictions on use of PHI in research and marketing
- raised the penalties for negligent disclosures

HIPAA Compliance Audits

The HITECH Act further requires DHHS to provide periodic audits to ensure that covered entities and business associates are complying with HIPAA Privacy and Security Rules and Breach Notification standards. The OCR has developed an audit program that is used to assess HIPAA privacy and security programs and compliance efforts. It examines mechanisms for compliance, identifies best practices, and discovers risks and vulnerabilities that may not be identified through other means. All covered entities, including health plans, health care clearinghouses, health care providers, and business associates, are eligible for an audit. Over the past decade, OCR audits have focused on how covered entities have implemented controls and processes to meet HIPAA Privacy and Security and Breach Notification Rules.

2.11 QUICK REVIEW
Question: Name three specific areas addressed in HITECH.

CONSEQUENCES OF NONCOMPLIANCE WITH HIPAA AND HITECH

Different governing bodies handle the prosecution of HIPAA violations. DHHS handles issues regarding transaction code sets and security. Complaints can be filed against a covered entity for not complying with these rules. The OCR oversees privacy issues and complaints and refers criminal issues to the **Office of the Inspector General (OIG)**. The OIG provides the workup for referral cases, which may involve the Federal Bureau of Investigation (**FBI**) and other agencies. Health care organizations are expected to have an active HIPAA compliance plan in place.

Since the 2003 HIPAA Privacy Rule compliance date, the OCR has investigated more than 231,968 complaints.[1] Sometimes the investigation finds that no violation occurred. When a violation has occurred, the OCR attempts to resolve the situation with one of the following:

- Voluntary compliance where the OCR may provide training and technical assistance to bring an entity into compliance;
- Corrective action where the OCR outlines a step-by-step process to correct the violation and ensure it does not happen again; and/or
- Resolution agreement where the covered entity is obligated to perform certain tasks and report to the OCR for 3 years. It often includes a monetary penalty.

Penalties for Noncompliance With the Provisions of HIPAA

There are both civil and criminal penalties for failure to comply with HIPAA regulations. The HITECH Act significantly increased the penalty amounts that may be imposed for violations related to failure to comply with HIPAA rules. These were initially established as follows:

- $100 to $50,000 if the covered entity did not know about the violation
- $1000 to $50,000 if the violation was due to reasonable cause
- $10,000 to $50,000 if the violation was due to willful neglect and was corrected
- $50,000 or more if the violation was due to willful neglect and was not corrected

All penalties have increased due to inflation each year.

The HITECH Act set a maximum penalty of $1.5 million for all violations of an identical provision in a calendar year. Penalties may also be applied on a daily basis if the OCR sees fit to do so. An example of when this may occur would be if a health

[1]Department of Health and Human Services. (2020, March 31). Enforcement Highlights. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

care organization refuses to give patients copies of their records when requested. In this case, OCR may apply the penalty per day that the organization was in violation.

Individuals also can be held personally responsible for HIPAA violations with criminal actions as follows:

- Knowing violations: up to $50,000 and/or 1 year in prison
- Misrepresentation or offenses under false pretenses: up to $100,000 and/or 5 years in prison
- Intent to sell, distribute, etc.: up to $250,000 and/or 10 years in prison

Refraining From Intimidating or Retaliatory Acts

HIPAA privacy regulations prohibit a covered entity from intimidating, threatening, coercing, discriminating against, or otherwise taking retaliatory action against individuals for any of the following:

- for exercising HIPAA privacy rights
- for filing a complaint with DHHS
- for testifying, assisting, or participating in an investigation, or
- for reasonably opposing any practice prohibited by the regulation.

Examples of Recent HIPAA Violations

In 2018, Anthem, Inc. was found to have had a breach exposing 78.8 million records. They agreed to a settlement of $16 million to settle the breach. This was the largest HIPAA settlement to date. They were found not only to have insufficient controls in place to prevent such a breach, but they also failed to respond adequately once the breach was detected.

Fresenius Medical Care North America had multiple recent HIPAA violations regarding stolen computers and unencrypted thumb drives. The company settled the case for $3.5 million. In addition to the monetary penalties, the company and all of its entities must conduct comprehensive risk analyses to address further areas of risk. P&P must be developed to address devices, media, and access controls.

The University of Texas MD Anderson Cancer Center was ordered to pay a civil monetary penalty of $4,348,000 to settle a case. The center had lost a laptop and two unencrypted thumb drives thereby exposing 34,883 patients' ePHI. Despite having P&P in place requiring all devices to be encrypted, the health center had failed to implement these policies until after the theft.

Massachusetts General Hospital was fined $515,000 for allowing film crews to record patients without consent for the TV series, Boston Med. The corrective action plan included additional staff training on allowable uses and disclosures of PHI to film and media.

In 2017, Memorial Healthcare System paid HHS $5.5 million and agreed to a corrective action plan to settle HIPAA violations. They self-reported to HHS a potential breach of PHI for over 115,000 patients. A former employee's login credentials had been used for a year to access patient records. HHS found that the organization had failed to review activity or terminate the former employee's access despite having identified this risk several years before the breach.

In January 2017, HHS announced the first settlement based on untimely breach notification. Presence Health in Illinois agreed to pay $475,000 and complete a corrective action plan when it failed to notify affected individuals within 60 days of discovering a breach. Though the notification was otherwise handled correctly, the OCR sent a clear message to other organizations. Every aspect of the HIPAA rules and Breach Notification Rules must be followed to the letter.

These and other OCR Resolution Agreements can be reviewed on the DHHS website (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html).

2.12 QUICK REVIEW

Question: Name four governing bodies that oversee or prosecute HIPAA violations.

ORGANIZATION AND STAFF RESPONSIBILITIES IN PROTECTING PATIENT RIGHTS

HIPAA affects all areas of the health care office, from the reception area to the provider (see Fig. 2.4). In addition to being educated and trained in job responsibilities, every staff member must be educated about HIPAA and trained in the P&P pertinent to the organization.

Obligations of the Health Care Organization

The covered entity must implement written P&P that comply with HIPAA standards. P&P are tailored guidelines established to inform each employee of their role within the organization. It is important that PHI is addressed in these guidelines. HIPAA requires each organization to implement P&P that comply with privacy and security rules. The organization should have a P&P manual to train providers and staff and to serve as a resource for situations that need clarification. Revisions to P&P must be made as needed and appropriate to comply with laws as they change. Documentation must be maintained in written or electronic form and retained for 6 years after its creation or when it was last in effect, whichever is later.

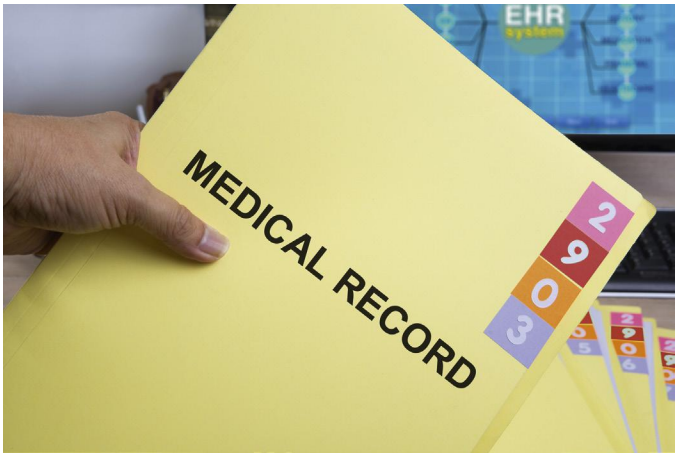

Fig. 2.4 Health Insurance Portability and Accountability Act (HIPAA), privacy, and security affect every level of the health care organization. (From iStock photo.com.)

HIPAA and Social Media

In 2020, there were approximately 3.8 billion social media users worldwide.[2] These social media users were spending almost two and a half hours per day on an average of eight social networking sites.[3] In addition to individual health care workers socializing on various sites, many health care organizations and providers use social media channels as a method of connecting with their patients and attracting new ones. As such, health care organizations must have a social media policy in place to ensure patient privacy is maintained. Training should be given to new employees as part of their orientation, and a refresher should be done annually to make sure the social media rules are not forgotten.

Under HIPAA's privacy rule, sharing protected health information on social media is prohibited. This includes any text, video or pictures that can potentially identify a patient. PHI can only be posted on social media with the patient's written consent outlining both the specific information that can be shared and specific purpose for using it.

Posting images or videos of patients without their consent is a HIPAA violation. This holds true if the patient is not the specific subject of the picture or video, but is simply in the frame, or if their PHI is visible. It is also a HIPAA violation if a health care worker posts gossip about a patient. Remember violations occur even if the patient is not listed by name but can be identified by the information shared.

Having conversations with patients on a health care organization's social media page can be an effective way of engaging them. Regardless of what a patient may share about themselves, it is important to protect their PHI. Violations can still occur even if the patient initiates the conversation. It is best to ask the patient to private message, email or call to continue the conversation.

Best Practices to Avoid Common HIPAA Violations

An insurance billing specialist will likely answer the telephone and speak during the course of their job, and there may be uncertainties about what questions they can and cannot answer. Reasonable and appropriate safeguards must be taken to ensure that all confidential health information is protected from unauthorized and inappropriate access, in both verbal and written forms (Fig. 2.5).

- Consider that conversations occurring throughout the office may be overheard. The reception area and waiting room are often linked and it is easy to hear the scheduling of appointments and exchange of confidential information. It is necessary to observe work areas and maximize efforts to avoid unauthorized disclosures. Simple and affordable precautions include using privacy glass at the front desk and having conversations away from settings where other patients or visitors are present. Health care providers can move their dictation stations away from patient areas or wait until no patients are present before dictating. Telephone conversations made by providers in front of patients, even in emergency situations, should be avoided. Providers and staff must use their best professional judgment.
- Be sure to check in both the patient's health record and the medical billing systems to determine whether there are any special instructions for contacting the patient regarding scheduling or reporting test results. Follow these requests as agreed by the office.
- Patient sign-in sheets are permissible but limit the information a patient is required to list when they sign in and change the sheet periodically during the day. A sign-in sheet must not contain information such as a reason for the encounter or the patient's medical condition. Because some providers specialize in treating patients with sensitive issues, simply showing that a particular individual has an appointment with the provider may pose a breach of patient confidentiality.
- Formal policies for transferring and accepting outside PHI must address how the health care organization keeps this information confidential. When using courier services, billing services, transcription services, or e-mail, transferring PHI must be done in a secure and compliant manner.
- Computers are used for a variety of administrative functions, including scheduling, billing, and managing health records. Computers are typically present at the reception area. Keep the computer screen turned so that viewing is restricted to authorized staff. Screen savers should be used to prevent unauthorized viewing or access. The computer should automatically log off the user after a period of being idle, requiring the staff member to reenter their password.

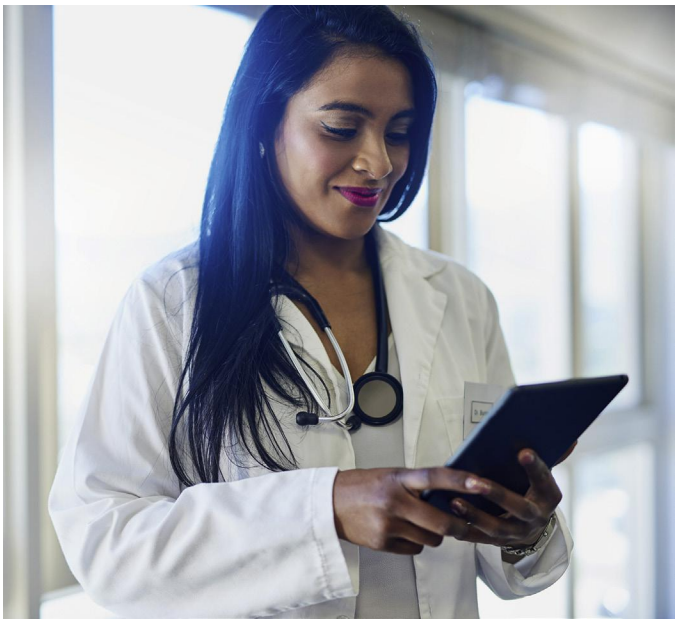

Fig. 2.5 Privacy and security must be considered in every aspect of a health care worker's job, from phone conversations to computer use to physical surroundings. (From iStock photo.com.)

[2]Market.US. (2020, April 17). Social Media Statistics and Facts. https://market.us/statistics/social-media/.

[3]Smart Insights. (2020, April 17). Global Social Media Research Summary 2020. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

- Keep usernames and passwords confidential and change them often. Do not share this information. An authorized staff member, such as the PO, will have administrative access to reset a lost or compromised password. Also, medical billing systems can track users and follow their activity. Safeguards include password protection for electronic data and storing paper records securely.
- Safeguard work areas; do not place notes with confidential information in areas that are easy to view by nonstaff. Cleaning services will access the building, usually after business hours; ensure that PHI is properly safeguarded.
- Place patient health records face down at reception areas so that the patient's name is not exposed to other patients or visitors. When placing health records on the door of an examination room, turn the chart so that identifying information faces the door. If medical charts are kept on countertops or in receptacles, it is important to ensure that nonstaff persons will not access the records.
- Do not post the health care provider's schedule in areas viewable by nonstaff individuals. Schedules are often posted for the convenience of the professional staff, but this may be a breach of patient confidentiality.
- Fax machines should not be placed in patient examination rooms or in any reception area where nonstaff persons may view incoming or sent documents. Only staff members should have access to the faxes.
- Health care workers who open office mail or take telephone calls pertaining to health record requests should direct these requests to the appropriate staff member.
- Exercise good judgment in writing and wording e-mails because they do not give security against confidentiality.
- Send all privacy-related questions or concerns to the appropriate staff member.
- Immediately report any suspected or known improper behavior to the supervisor or the PO so that the issue may be documented and investigated. Any questions about policies and procedures should be directed to the PO (Fig. 2.6).
- Never discuss patients casually with co-workers, friends, or family. Be mindful of the surroundings. Avoid sharing any patient information on social media. Even if a patient is not mentioned by name, someone may recognize the patient.
- Do not respond to inquiries about a patient no matter how well meaning they may seem. Many people who do not work within the health care system are unaware that this is a HIPAA violation.
- Electronic files can be accessed on stolen or misplaced computers and smartphones. Home computers that do not have appropriate security may be easily hacked. Even texting can be hacked so it is important to only use phones to transmit patient data over secure applications that use encryption.
- Do not access health records for patients out of curiosity or as a favor to a family member or friend. Health care workers are allowed the minimum amount of access necessary to do their job. This is a common HIPAA violation that costs health care organizations every year.

Fig. 2.6 Insurance billing specialist consulting with the supervisor or office manager about office policies regarding release of a patient's health record.

Under HIPAA, health care providers and their employees are required to protect PHI and limit the use of it to the minimum amount necessary. Applying HIPAA requirements can be a challenge and penalties for violating HIPAA are high. Health care workers have an obligation to their employer and to the patients they serve.

Compliance is an ongoing effort involving teamwork. Health care workers should monitor their own activities to ensure that they are following the required protocols. Shortcuts cannot be taken when patient privacy and security are involved.

DISCUSSION POINT

Discuss various ways an insurance billing specialist can prevent HIPAA violations.

PROCEDURE 2.1 Understanding the Notice of Privacy Practices

Go to the following websites and answer the questions below.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/privacy-practices-for-protected-health-information/index.html

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf

1. Name three types of covered entities that are not required to develop an NPP.
2. Describe the four main areas of content that must be provided in the NPP.
3. When must a health plan provide an NPP?
4. When must a health care provider give notice?
5. If a patient requests a change to their health record, is the provider obligated to change it?
6. How long does a health care provider have to provide a copy of a patient's health information if it is requested?
7. If a patient requests a list of times their information was shared, how far back must the list go?
8. Name three ways a patient may file a complaint if they feel their rights have been violated?

KEY POINTS

This is a brief chapter review of the key issues presented. To further enhance your knowledge of the technical subject matter, review the key terms and key abbreviations for this chapter by locating the meaning for each in the Glossary at the end of this text, which appears in a section before the Index.

1. The Health Insurance Portability and Accountability Act (HIPAA) has affected confidentiality and disclosure of protected health information (PHI) and completion and electronic transactions in health care. It has also affected how health care organizations address fraud and abuse in claims submission and implementation of compliance and practice standards.
2. While employed by a health care organization, the insurance billing specialist's duty is to have complete knowledge and understanding of HIPAA mandates. Always carry out policies and procedures that comply with federal regulations, and keep up to date with these statutes. This will assist both the provider and the patients.
3. The primary purpose of HIPAA *Title I: Health Insurance Reform* is to provide continuous insurance coverage for workers and their insured dependents when they change or lose jobs. *Title II: Administrative Simplification* focuses on the health care organization setting and aims to reduce administrative costs and burdens.
4. Serious civil and criminal penalties, such as fines and imprisonment, apply for HIPAA noncompliance.
5. *PHI* refers to data that identify an individual and describe their health status, age, sex, ethnicity, or other demographic characteristics, whether that information is or is not stored or transmitted electronically.
6. Under HIPAA, PHI may not be used or disclosed without permission from the patient or someone authorized to act on behalf of the patient. Use or disclosure is permitted if it is specifically required for treatment, payment, or routine health care operations (TPO). The two types of disclosure required by the HIPAA Privacy Rule are to the individual who is the subject of the PHI and to the Secretary of the DHHS to investigate compliance with the rule.
7. *Disclosure* means the release, transfer, provision of access to, or divulging information to a person or entity outside the health care organization. *Use* means the sharing, employment, application, utilization, examination, or analysis of IIHI within an organization that holds such information. When a patient's billing record is accessed to review the claim submission history, the individual's health information is in use.
8. When comparing privileged and nonprivileged information, privileged information is related to the treatment and progress of the patient. The patient must sign an authorization to release this information or selected facts from the health record. Nonprivileged information consists of ordinary facts unrelated to treatment of the patient, including the patient's name, city of residence, and dates of admission or discharge.
9. Under HIPAA, a Notice of Privacy Practices (NPP) document must be given to the patient at the first encounter or at enrollment. The NPP explains the individual's rights and the health care organization's legal duties regarding PHI. Use and disclosure of PHI is permissible for TPO because the NPP describes how PHI is used for these purposes. Thus, a consent form is not required. The health care organization is required to obtain a signed authorization form to use or disclose health information for situations beyond the TPO. This is a protection for the health care organization. Psychotherapy notes are handled separately under HIPAA. Such notes have additional protection, specifically that an authorization for any disclosure of psychotherapy notes must be obtained.
10. The three major categories of security safeguards are administrative, technical, and physical measures that will reasonably protect PHI from any use or disclosure that is in violation of HIPAA.
11. DHHS and the OCR perform HIPAA audits and place substantial fines on covered entities that do not follow HIPAA regulations.

Strongly consider the lessons learned from the privacy, transaction, and security rules in conjunction with OIG compliance recommendations. The most important points are to read the health care organization's P&P manual and to ask questions about the general operations of the organization. Always use the best practice approach to be an informed and effective employee.

INTERNET RESOURCES

OIG HIPAA for Professionals Compliance Enforcement

- https://www.hhs.gov/hipaa/for-professionals/compliance enforcement/agreements/index.html.

OIG HIPAA for Professionals NPP Guidance

- https://www.hhs.gov/hipaa/for-professionals/privacy /guidance/privacy-practices-for-protected-health -information/index.html.

OIG HIPAA for Professionals Model NPP

- https://www.hhs.gov/hipaa/for-professionals/privacy /guidance/model-notices-privacy-practices/index.html.

OIG HIPAA for Professionals Sample NPP for Health Care Providers

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa /npp_fullpage_hc_provider.pdf.

STUDENT ASSIGNMENTS

- Study Chapter 2.
- Complete all exercises all in the *Workbook* to reinforce the theory learned in this chapter.
- Turn to the Glossary at the end of this text for a further understanding of the key terms and key abbreviations used in this chapter.

3

Compliance, Fraud, and Abuse

Cheryl Fassett

OBJECTIVES

After reading this chapter, you should be able to:

1. Define compliance.
2. Discuss the difference between fraud and abuse.
3. List examples of fraud and abuse in the health care setting.
4. Identify the federal and state laws that regulate health care fraud and abuse.
5. Understand the penalties for fraud and abuse.
6. Identify the various fraud and abuse audit programs.
7. Discuss the basic components of an effective compliance program.
8. Discuss potential risk areas for provider groups, billing companies, and hospitals.

KEY TERMS

abuse
Anti-Kickback Law
assumption coding
auditing
Civil False Claims Act
Civil Monetary Penalty
Clinical Laboratory Improvement Amendments
clustering
compliance
compliance plan
Comprehensive Error Rate Testing
corrective action plan
cost reports
Criminal False Claims Act
DRG upcoding/DRG creep
embezzlement
Emergency Medical Treatment and Labor Act
Exclusion Statute
Federal Deposit Insurance Corporation
fraud
Fraud Enforcement and Recovery Act
Health Care Fraud and Abuse Control
Health Care Fraud Prevention and Enforcement Action Team
kickback
medical necessity
Medicare Administrative Contractor
Medicare Integrity Program
monitoring
Occupational Safety and Health Administration
Office of Inspector General
OIG Work Plan
Operation Restore Trust
patient dumping
phantom bills
Physician Self-Referral Law
qui tam
Recovery Audit Contractor
safe harbor
Self-Disclosure Protocol
Stark Law
undercoding
upcoding
Zone Program Integrity Contractor

KEY ABBREVIATIONS

CERT
CLIA
CMP
CMS
DHHS
DOJ
EMTALA
FCA
FDIC
FERA
HCFAC
HEAT
MAC
MIP
OIG
ORT
OSHA
P&P
PPACA
RAC
SDP
ZPIC

INSIGHTS FROM THE FIELD

Lisa N.: Certified Professional Coder (CPC), Certified Professional Compliance Officer (CPCO), Certified Documentation Expert - Outpatient (CDEO), Certified Professional Mediacl Auditor (CPMA), Certified Risk Adjustment Coder (CRC), Certified Professional Coding - Instructor (CPC-I)

I have worked in health care for 40 years! I started as a medical assistant, but have been a biller, coder, reimbursement specialist, physician educator, and held various department and practice management positions over the years. I am currently a corporate compliance advisor. I educate providers and perform annual reviews to ensure correct coding and documentation. When I started in medicine, you were able to learn on the job—you didn't have to have any degrees or certifications to get a job in a medical office. Along the way, I was able to get certifications to make me more valuable to my employers. Learning all the guidelines, rules, codes, and so on is challenging enough, but that really doesn't prepare you to be able to interact with providers. Providers can have strong personalities, and I advise you to have a thick skin and hold your ground. Look them in the eye, be professional, and ALWAYS get back to them with an answer to their question. I never have a problem telling a provider that I don't know the answer, but you can bet I'll follow up and let them know. It's okay to admit we don't know it all, but they need to have confidence that you will find out.

COMPLIANCE DEFINED

Health care is one of the most highly regulated industries, holding the health care worker to the highest levels of scrutiny. Any individual working in health care and any business that is involved with the health care industry must conform to the principles and practices identified by state and federal agencies.

Compliance in the health care industry is the ongoing process of meeting regulations, recommendations, and expectations of federal and state agencies that pay for health care services and regulate the industry (Fig. 3.1). Health care compliance involves the following:

- The claims reimbursement processes
- Managed care procedures
- Protection of patients' privacy
- Various guidelines and statutes
- Licensure
- Patient safety
- Attention to the law

A compliance plan outlines the organization's standardized process for handling business functions, much like a user's manual. This will enable consistent and effective management and staff performance.

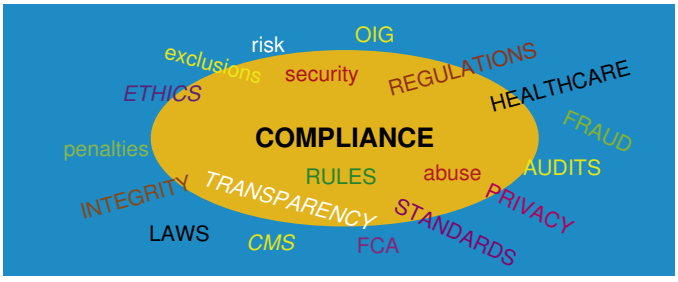

Fig. 3.1 Compliance involves many players, laws, and standards. A compliance plan is a set of policies, procedures, and guidelines to ensure an organization conducts its business in accordance with applicable laws and regulations.

The first step toward achieving compliance is understanding the laws that regulate the industry. Failure to comply with the associated mandates can lead to criminal penalties and/or civil fines.

3.1 QUICK REVIEW

Question: What is compliance?

FRAUD AND ABUSE LAWS

The US Department of Justice (**DOJ**), tasked with prosecuting health care fraud and abuse cases, announced that it recovered $2.6 billion in health care fraud in 2019 alone, up from both preceding years.[1] With many regulations and laws in place, there are very tight controls on medical billing. All individuals involved in the provision of health care services and in billing for those services are held to very high standards. Considering complex government regulations and constant scrutiny, it is important for those involved in the reimbursement process to clearly understand fraud and abuse. Both fraud and abuse can expose providers, health care organizations, and heath care workers to criminal and civil liability.

Fraud can occur when deception is used in claim submission to obtain payment from the payer. Individuals who knowingly, willfully, and intentionally submit false information to benefit themselves or others commit fraud. Fraud can also be seen in mistakes that result in excessive reimbursement. It is not necessary to prove intent to defraud. Liability can occur when a person knowingly presents or makes a false record that creates a false claim.

As you will learn later in this textbook, insurance claims require codes that describe what was wrong with the patient (diagnosis codes) and what service was provided to the patient (procedural codes). Codes must be reported accurately on claim forms. A fraudulent claim may be one that has been coded to maximize payment by reflecting a higher service level. An inaccurate diagnosis may be billed to justify a service that was not medically necessary. A claim may also be filed for services that never took place, or for a patient who was never seen. Patients can also commit fraud by stealing a person's identity and using their insurance coverage, or providing false information on their health insurance applications. Further examples of health care fraud are listed in Box 3.1.

Abuse describes incidents or practices by health care organizations, not usually considered fraudulent, that conflict with accepted sound medical business or fiscal practices. An example of abuse in billing practices may be to submit excessive charges for services or supplies, or duplicate billing. Additional examples of health care abuse are listed in Box 3.2.

[1]Office of Public Affairs, Department of Justice. (2020, January 9) Justice Department Recovers over $3 Billion from False Claims Act Cases in Fiscal Year 2019. https://www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019.