15TH EDITION

FORDNEY'S Medical Insurance

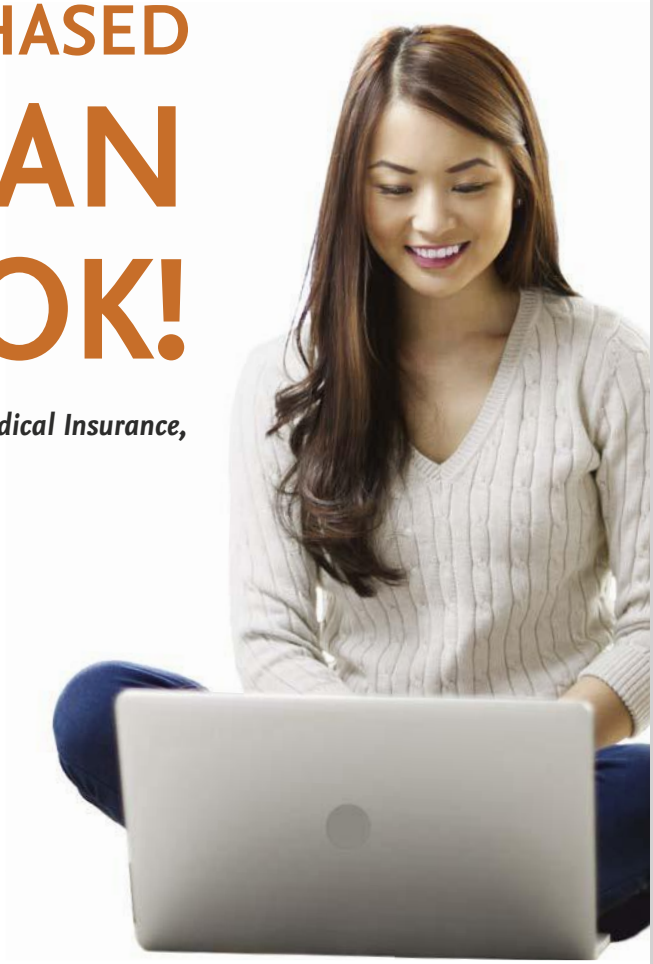
LINDA M. SMITH

Evolve® | Student Resources on Evolve
Access Code Inside

ELSEVIER

Evolve®

YOU'VE JUST PURCHASED MORE THAN A TEXTBOOK!



Evolve Student Resources for *Smith: Fordney's Medical Insurance, 15th Edition*, include the following:

- SIM Chart for the Medical Office Activities
- Performance Evaluation Checklists
- Interactive UB-04 Form Filler
- Self-Assessment Quizzes
- Forms and Documents

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 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.

2018v1.0

FORDNEY'S

Medical Insurance

This page intentionally left blank

15TH EDITION

FORDNEY'S
Medical Insurance

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

FORDNEY'S MEDICAL INSURANCE,
FIFTEENTH EDITION

ISBN: 978-0-323-59440-0

ISBN: 978-0-323-59440-0

Publishing Director: Kristin Wilhelm
Senior Content Strategist: Linda Woodard
Senior Content Development Manager: Ellen Wurm-Cutter
Senior Content Development Specialist: Maria Broeker
Publishing Services Manager: Deepthi Unni
Senior Project Manager: Kamatchi Madhavan
Project Manager: Haritha Dharmarajan
Designer: Renee Duenow

Printed in Canada

ELSEVIER

3251 Riverport Lane
St. Louis, Missouri 63043

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 progressed through health care, 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 18 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). She is a frequent presenter at AAPC chapter events in New York State. 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 fifteenth edition.

ACKNOWLEDGMENTS

I would like to acknowledge and dedicate this fifteenth 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 thirteenth and fourteenth editions of the *Handbook*, but truly an honor to be asked to follow in Marilyn's footsteps as the primary editor of this fifteenth edition. 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 contributor in eight chapters of this fifteenth 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.

Thank you to contributors Nanette Sayles and Rachael D'Andrea, who have brought their experience and expertise in facility billing to update the *Insurance Handbook*. Their diligence in meeting deadlines and doing an excellent job is greatly appreciated.

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. 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. I express special appreciation to Maria Broeker, senior content development specialist, and Linda Woodard, senior content strategist, 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

CONTRIBUTORS AND REVIEWERS

CONTRIBUTORS

Rachael D'Andrea, MS, RHIA, CPHQ, CDIP, CHTS-TR
Professor, Health Information Management
Lake Sumter State College, Leesburg, Florida
Professor, Health Information Management and Health Care Administration
Charter Oak State College
New Britain, Connecticut

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

Nanette Sayles, EdD, RHIA, CCS, CHPS, CHDA, CPHI, CPHIMS, FAHIMA
Associate Professor, Health Information Management
East Central College
Union, Missouri

14TH EDITION EDITORIAL REVIEW BOARD

Sandra Alexander, MPA, BAS, CMA (AAMA)
Program Director/Coordinator, El Centro College, Dallas, Texas

Deborah A. Balentine, MEd, RHIA, CCS-P, CHTS-TR
Adjunct Instructor, Truman College, City College of Chicago, Chicago, Illinois

Kimberly, Head, DC
Director of Healthcare Programs, Continuing Education Health Sciences, Collin College, Plano, Texas

Geri Kale-Smith, MS, CMA
Coordinator, Medical Office Programs, Associate Professor, Health Careers Division, Harper College, Palatine, Illinois

Colleen O. Kim, BS
Certified SHIP Counselor, Senior Management Fraud Counselor, Adjunct Professor, Manchester Community College, Manchester, Connecticut

Jennifer K. Lester, RBA, CMAA, CBCS
Certified Allied Health Instructor, Adjunct Instructor, Charleston Jobs Corps Center, Kanawha Valley Community & Technical College, Charleston, West Virginia

Michelle C. Maus, MBA
Program Chair/Assistant Professor of Healthcare Administration, Tiffin University, Tiffin, Ohio

PREVIOUS EDITION REVIEWERS

Pamela Audette, MBA, MT(ASCP), RMA
Assistant Professor and Program Director, Finlandia University, Hancock, Michigan

Megan Baez, CPC, CMA (AAMA)
Medical Coding & Billing Instructor, Everest University, Lakeland, Florida

Kelly Berge, MSHA, CPC, CBCS
Assistant Dean, Online, Berkeley College, Clifton, New Jersey

Ruth Berger, MS, RHIA
Instructor, Health Information Technology, Chippewa Valley Technical College, Eau Claire, Wisconsin

Peggy Black, RN, CCS, AHIMA-Approved ICD-10-CM/PCS Trainer
Medical Coding and Billing Instructor, Winter Park Tech, Winter Park, Florida

Carrie Cosson, CMA (NCCT), RMA (AMT)
Medical Assisting Instructor, Everest University, Lakeland, Florida

Gerard Cronin, DC, CCA
Assistant Professor, Salem Community College, Carneys Point, New Jersey

Brian Edward Dickens, MBA, RMA, CHI
Program Director–MA, Southeastern College, Greenacres, Florida

Jennifer Flippin, CPC
Medical Billing and Coding Program Coordinator, Pinnacle Career Institute, Kansas City, Missouri

Carol Hendrickson, MS Ed, CCS-P
Medical Coding & Health Information Management Instructor, Pasco Hernanado Community College, New Port Richey, Florida

Mary A. Johnson, BA, CPC
Program Manager, Medical Record Coding, Central Carolina Technical College, Sumter, South Carolina

Judith Leonhart, MBA
Instructor, Adult Education, OCM BOCES, Liverpool, New York

Angela MacLeod, MS, RHIA
Medical Coding & Billing Instructor, Certified Medical Assistant Program Director, Gogebic Community College, Ironwood, Michigan

Cassondra Major, MBA
Academic Program Director, Medical, Everest College, Henderson, Nevada

JanMarie C. Malik, MBA, RHIA, CCS-P
Coding, Billing, Reimbursement, and Office Procedures Instructor, Shasta Community College; National University, Redding, California

Laura Melendez, BS, RMA, RT BMO
Allied Health Instructor, Medical Assisting, Southeastern College, Greenacres, Florida

Deborah Newton, MA, PhD
Program Director, Medical Billing/Coding, Great Falls College Montana State University, Great Falls, Montana

Bhamini Patel, BSHIM, CPC, CPC-H
Medical Coding and Billing Instructor, Everest University, Lakeland, Florida

Jeanice Porta, BSEd, CPC, CPC-I
Medical Coding/Billing Instructor, Lee County High Tech Center North, Cape Coral, Florida

Susan Shear, MHA, CPC
Assistant Professor, Medical Information Technology, Bluegrass Community and Technical College, Danville, Kentucky

Tara Shepherd, CMA (AAMA)
Allied Health Director, Apollo Career Center, Lima, Ohio

Phaedra Spartan, RMA, CMAS, BS, MSHA
Healthcare Programs, Director, Medical, Vatterott College, Springfield, Missouri

Mia K. Thompson, MIBC, MAA
Program Director, Everest Institute, Marietta, Georgia

Deanne Ulrich, CPC-A
Instructor, Business, Hawkeye Community College, Waterloo, Iowa

Chris Welch, MBA, CPC, CMC, CEC, CMPE
Medical Insurance Billing and Coding, Program Director, Everest University, Orange Park, Florida

Nancy C. Withee, CPC, CPMA
Program Coordinator, Medical Office Administration and Health Information Technology, Great Bay Community College, Portsmouth, New Hampshire

WELCOME TO THE FIFTEENTH EDITION

Marilyn Fordney first published the *Insurance Handbook* in 1977. At that time, few people were aware of how important the subject of health insurance would become. The *Insurance Handbook* now celebrates its fifteenth year. 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. The longevity of this publication speaks for itself, and through the years, Fordney's *Insurance Handbook* has become the leader in its field. The *Handbook* is widely accepted across the nation among educators and working insurance billing specialists and coders.

Because of the ever-changing nature of health care, putting the fifteenth edition together has been challenging and exciting. Because changes occur daily in the insurance industry, the *Insurance Handbook* is revised every 2 years to keep the information current.

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 physician's business: insurance coding and billing.

Why Is This Book Important to the Profession?

In the past two 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 the *Handbook* 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 have 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. The *Handbook* 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 medical practices, and maintain a good relationship with patients. Even offices 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 physician's office 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 physician's office. The *Insurance Handbook* may be used as a learning tool and resource guide in all of those programs as well as in vocational or commercial training institutes and welfare-to-work programs. The *Insurance Handbook* also serves as a text for in-service training in the private medical office. The *Handbook* may 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 the *Handbook* to be a valuable reference tool when answering clients' questions.

Originally the *Handbook* was designed primarily for students who plan to seek employment in an outpatient setting (such as a physician's office or clinic). To keep pace with the ever-changing health care environment, the fifteenth edition has added a section for billing in the ambulatory surgical center setting. Furthermore, the fifteenth edition of the textbook has been expanded to provide a strong foundation of knowledge to students who may seek employment in the hospital inpatient setting.

Because of the strong base of knowledge that the insurance billing specialist will need to understand the federal guidelines associated with our industry, the fifteenth edition has designated two separate chapters to address them in depth. The student will receive a thorough understanding of compliance issues associated with privacy, security, and the Health Insurance Portability and Accountability Act in Chapter 2 of the textbook. Chapter 3 will provide an in-depth training in the essentials of compliance related to health care fraud and abuse.

Many types of insurance coverage are available in the United States. In Unit 2 of the *Handbook* (Introduction to Health

Insurance), the types most commonly encountered in physicians' offices and clinics have been emphasized in simple, nontechnical explanations and tables.

Over the years, medical documentation and the electronic health record have become essential components of the medical billing process. The insurance billing specialist must be knowledgeable of documentation requirements to assist providers and to ensure compliance in billing. In recent years the federal government targeted this issue with the introduction of Medicare compliance policies related to documentation; such issues are therefore covered to help physicians comply with possible reviews or audits of their billing practices. A strong emphasis has also been placed on the diagnostic and procedural chapters of the textbook. Finally, the *Handbook* 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 physician and his or her insurance billing specialist should always seek legal counsel about specific questions of law as they relate to medical practice.
- Compliance Alerts are interspersed throughout all chapters for emphasis.

! COMPLIANCE ALERT

- 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; spellouts 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. 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:

PROPERTY AND CASUALTY CLAIMS

All payer guidelines, including all private insurance companies and all federal and state programs.

MEDICAID

State Medicaid programs.

MEDICARE

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

TRICARE

TRICARE Standard (formerly CHAMPUS), TRICARE Prime, and TRICARE Extra.

CHAMPVA

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

WORKERS' COMPENSATION

State workers' compensation programs.

MANAGED CARE

All managed care organizations.

MATERNAL AND CHILD HEALTH PROGRAM

State and federal program for children younger than 21 years of age and with special health needs.

Disability Income Insurance

Insurance programs that replace income lost as a result of illness, injury, or disease.

CONSUMER-DIRECTED HEALTH PLANS

Self-directed health plans that often pair a high-deductible preferred provider organization (PPO) plan with a tax-advantaged account.

INDEMNITY HEALTH INSURANCE

Traditional or fee-for-service health plans.

ORGANIZATION

- Chapters 1 through 3 explain the role of the insurance billing specialist and provide them with a thorough understanding of the associated responsibilities. Legislation related to health care and the federal guidelines that affect our industry are laid out for the student. This is coupled with a strong emphasis on the compliance process and their obligation to comply in all situations. Chapters 4 through 10 will provide the student with an introduction into health insurance. These chapters will provide the basics of health care and introduce readers to the various types of insurance carriers they will more than likely need to be familiar with. 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.
- Chapters 11 to 13 contain information related to medical documentation and the electronic health record that is critical for the insurance billing specialist to understand. The student will learn and develop diagnostic coding and procedural coding skills. Chapters 14 and 15 will teach students the claims submission process. The textbook offers a unique block by block approach to completion of an insurance claim form.
- A new unit (5) has been added in the fifteenth edition, titled Revenue Cycle Management, and includes Chapters 16 and 17. These chapters focus on the skills necessary to receive payment 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 of the *Handbook,* which covers facility billing, has been expanded. Chapter 18 is new to the textbook to introduce the student to ambulatory surgical centers (ASCs) and the challenges of billing for this newer type of facility. The chapter outlines the process for billing in the ASC setting. Chapter 19, Hospital Outpatient and Inpatient Billing, is intended especially for those students interested in pursuing a career in the hospital setting. It presents information about the *International Classification of Disease, Tenth Revision, Procedure Classification System (*ICD-10-PCS). Additionally, step-by-step procedures are stated for processing a new patient for admission and to verify insurance benefits. It has been updated to provide the most current issues impacting insurance billing specialists in the hospital setting.
- Chapter 20, "Seeking a Job and Attaining Professional Advancement," provides information pertinent to seeking a position as an insurance billing specialist, a self-employed claims assistance professional, or an electronic claims processor using high-tech procedures. The chapter explains career advancement and certification opportunities for the insurance billing specialist.

ANCILLARIES

Workbook

Users of the *Workbook* that accompanies this edition of the textbook will find the following features:

- Competency-based education is discussed. A point system has been applied to code and claims completion for *Workbook* assignments for instructors who need to document and gather statistics for competency-based education. The worksheets for each assignment are available on the Evolve website. *Textbook* learning objectives, *Workbook* performance objectives for all assignments, use of the tutorial software with reinforcement by *Workbook* assignments, the test section at the end of the *Workbook*, the quizzes of key terms featured on the website, and incorporation of classroom activities and suggestions from the *TEACH Instructor's Resource Manual* (available on the companion Evolve website) provide a complete competency-based educational program.
- Self-assessment quizzes for each chapter are available on the Evolve website for student use.
- Patient records and ledgers have been updated and reworded to correspond with the 2018 procedural codes and ICD-10-CM diagnostic code books.
- All chapters have fill-in-the-blank, multiple-choice, mix-and-match, and true/false review questions. Answers have been put into the *TEACH Instructor's Resource Manual* (available on the companion Evolve website).

General Features

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. Chapter outlines serve as a lecture guide. 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' spellouts. Patients' medical records, financial accounting statements, and encounter forms are presented as they might appear in the physician'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 2018 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. Insurance claim forms and letterheads are available on the Evolve website. Some assignments give students hands-on experience in keying insurance claims on the CMS-1500 claim forms using standardized guidelines developed by the National Uniform Claim Committee. Current procedural and diagnostic code exercises are used throughout the *Workbook* to facilitate and enhance coding skills for submitting a claim or posting to a patient's financial account statement. Critical thinking problems are presented in each chapter. 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).

Student Software Challenge (Located on Evolve)

The Student Software Challenge ICD-10 located on Evolve is user-friendly software that provides students with another opportunity for hands-on learning. This software simulates a realistic experience by having students gather necessary documents and extract specific information to complete the CMS-1500 insurance claim form. All source documents appear on screen and may be viewed simultaneously in a separate window. The Student Software Challenge also allows users to print the claim form for evaluation and edit it to correct errors.

The main objective is to complete CMS-1500 forms for each case and insert accurate data, including diagnostic and procedural code numbers. Instructors may want their students to work through the first case or basic cases (1 through 4) strictly for learning and to use Case 5 for testing and grading. Cases 6 through 10, which are advanced and insurance specific (for example, Medicare, TRICARE), may be used for practice or testing. This simulated learning methodology makes possible an easier transition from classroom to workplace.

Additional features of the Student Software Challenge for the fifteenth edition of this textbook include the following:

- Blank interactive forms that can be typed into and printed or saved to be turned in to the instructor. This creates clean claims that are easier to read and grade.
- Complete fee schedule to simplify the insertion of fees on the CMS-1500 claim form or financial accounting record.

Other Student Evolve Resources

In addition to the Student Software Challenge, students also have access to an interactive UB-04 form filler and various documents and forms. Also included are insurance cases to accompany SIM Chart for the Medical Office, which is a simulated online EHR.

TEACH Instructor's Resource Manual (Located on Evolve)

The *TEACH Instructor's Resource Manual* is available on the Evolve site; it contains lesson plans, *Workbook* answer keys, a test bank, and PowerPoint slides. 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:

- Guidelines for establishing a medical insurance course
- 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
- Lesson plans for each chapter
- Suggested classroom activities and games
- Ideas on how to use the text as an adjunct to an administrative medical assisting or medical office procedures course
- Pretests for each chapter

Evolve Companion Website

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

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:

- Self-assessment quizzes 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.
- Technical updates to keep up with changes in government regulations and codes as well as other industry changes.
- SimChart for the Medical Office application cases focused on the Billing and Coding module. SCMO customers can utilize this resource to reinforce practice management and EHR skills.
- Performance Evaluation Checklists.

Elsevier Adaptive Learning (Additional Purchase Required)

Elsevier Adaptive Learning is a uniquely personalized and interactive tool that enables students to learn faster and remember longer. It's fun; it's engaging; and it's constantly tracking student performance and adapting to deliver content precisely when it's needed to ensure information is transformed into lasting knowledge.

- Greater student performance
- Long-term knowledge storage
- Individualized learning
- Cognitive skills training
- Time management Dashboards and reporting
- Mobile app

SUMMARY

The *Handbook* and its ancillaries provide a complete competency-based educational program. *Handbook* learning objectives, *Workbook* 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 rapid increase of managed care plans 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

UNIT 2 Introduction to Health Insurance

This page intentionally left blank

FORDNEY'S

Medical Insurance

This page intentionally left blank

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 responsibilities assigned to insurance billing and coding specialists and electronic claims processors.
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. State the personal image to be projected as an insurance billing specialist.
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

American Medical Association
cash flow
claims assistance professional
claims examiners
cycle
electronic mail
errors and omissions insurance
ethics
etiquette
facility billing
independent contractor
insurance billing specialist
list service
medical billing representative
professional billing
reimbursement specialist
respondeat superior
revenue
self-pay patient
senior billing representative

KEY ABBREVIATIONS

AMA
ASHD
CAP
e-mail
listserv
MSO
NPP

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, some of the basic words in this and subsequent chapters appear in **bold** or *italic* type.

Medical insurance billing specialists' primary goal is to assist in the revenue cycle, both helping the patient to obtain maximum insurance plan benefits and ensuring a cash flow to the health care organization they are employed by. **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 very complex. The charge for a baby being born in the late 1960s probably was as little as $250. It was probably a flat fee that covered a 3-day hospital stay and a doctor's fee. The receipt for the birth probably 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 cost for giving birth can run to more than $37,000 for an uncomplicated delivery and nearly double that for a cesarean delivery. 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. The billing is performed using a computer, patient conditions and services must be coded, and there are a variety of methods

of reimbursement for the services. 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 very 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 physicians, and co-workers.

Two billing components exist: 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. Whether you are employed to perform facility or professional billing functions, 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. You 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 patients' visits. 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 visit must also be produced. It is important to record why the patient requires a visit.
- *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 back-office procedures and submission and payment of claims.
- *Documenting* pertinent clinical notes and assigning a diagnosis and service code to the patient's condition and visit is done by the provider of service. The notes in the patient's health record include the reason for the visit, 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 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 visit 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.

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; 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, you should be able to perform any and all duties assigned pertaining to the business office. Front and back office personnel work together to ensure a strong revenue cycle and enhanced reimbursement. Examples of generic job descriptions are shown in Figs. 1.1 and 1.2 to illustrate the job duties, skills, and requirements that might be encountered for various insurance billing and coding positions.

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 practice's financial policies and review the patient's insurance coverage. The counselor confirms the deductible or copayment amount and verifies with the insurance company 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 visit before the patient is treated.

After the patient has been treated, documentation of services should be confirmed as completed. Documentation of services is vital to good patient care and must be done comprehensively for proper reimbursement. A coding specialist may review diagnostic and procedural coding to ensure that the codes are supported in the documentation and that they are correct.

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; however, 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 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. 1.3).

Having large accounts receivables (total amount of money owed for health care services rendered) in a health care organization is often a direct result of failure to verify insurance plan benefits, obtain authorization or precertification, or collect copayments and deductibles 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.

The curriculum that might be offered in a 1-year certificate program for a medical insurance specialist is shown in Fig. 1.4. Courses in your locale are labeled with different titles and time frames; the information in Fig. 1.4 is specifically from a community college in Pennsylvania. 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 your goal is to become a self-employed insurance billing specialist or CAP. In addition to insurance terminology, claims procedures, and coding, you must know commercial insurance payers' requirements as well as Medicare and state Medicaid policies and regulations. You also need proficiency in running a business, including marketing and sales expertise.

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, employment in the field is expected to grow faster than jobs in other

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. Certified Procedural Coder (CPC) or Certified Coding Specialist (CCS) status preferred.

Working conditions:
Medical office setting. Sufficient lighting.

Physical demands:
Prolonged sitting, standing, and walking. Use of word processor or computer equipment. Some stooping, reaching, climbing, and bending. Occasional lifting of _____ lbs to a height of 5 feet. Hearing and speech capabilities necessary to communicate with patients and staff in person and on telephone. Vision capable of viewing computer monitors, calculators, charts, forms, text, and numbers for prolonged periods.

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 and physiology, diseases, surgeries, and medical specialties. 1.2 Consults reference materials to clarify meanings of words. 1.3 Meets accuracy and production requirements adopted by employer. 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.

Fig. 1.1 Generic job description for an insurance billing specialist.

Continued

3. Operates computer to transmit insurance claims.	3.1 Operates equipment skillfully and efficiently. 3.2 Evaluates condition of equipment and reports need for repair or replacement.
4. Follows employer's policies and procedures.	4.1 Punctual work attendance and is dependable. 4.2 Answers routine inquiries related to account balances and dates insurance forms submitted.
5. Transmits insurance claims accurately.	5.1 Updates insurance registration and account information. 5.2 Processes payments and posts to accounts accurately. 5.3 Handles correspondence related to insurance claims. 5.4 Reviews encounter forms for accuracy before submission to data entry. 5.5 Inserts data for generating insurance claims accurately. 5.6 Codes procedures and diagnoses accurately. 5.7 Telephones third-party payers with regard to delinquent claims. 5.8 Traces insurance claims. 5.9 Files appeals for denied claims. 5.10 Documents registration data from patients accurately. 5.11 Maintains separate insurance files.
6. Enhances knowledge and skills to keep up to date.	6.1 Attends continuing education activities. 6.2 Obtains current knowledge applicable to state and federal programs as they relate to insurance claim submission. 6.3 Keeps abreast and maintains files of current changes in coding requirements from Medicare, Medicaid, and other third-party payers. 6.4 Assists with updating fee schedules and encounter forms with current codes. 6.5 Assists in the research of proper coding techniques to maximize 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 regarding payment policies and financial obligations. 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. 7.6 Assists with giving fee estimates to patients when necessary.

Fig. 1.1, cont'd.

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. Certified Electronic Claims Processor (CECP) status preferred.

Working conditions:
Medical office setting. Sufficient lighting.

Physical demands:
Prolonged sitting, standing, and walking. Use of computer equipment. Some stooping, reaching, climbing, and bending. Occasional lifting of _____ lbs to a height of 5 feet. Hearing and speech capabilities necessary to communicate with patients and staff in person and on telephone. Vision capabilities necessary to view computer monitors, calculators, charts, forms, text, and numbers for prolonged periods.

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 and physiology, 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 to clarify meanings of words. 1.4 Meets accuracy and production requirements adopted by employer. 1.5 Verifies with physician any vague information for accuracy. 1.6 Reduces volume of paperwork and variety of claim forms providers need to submit claims for payment.
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 account balances and dates insurance data transmitted to third-party payers.

Fig. 1.2 Generic job description for an electronic claims processor.

Continued

	2.3 Updates and maintains software applications with requirements of clearinghouses and third-party payers.
3. Uses software that eliminates common claim filing errors, provides clean claims to third-party payers, expedites payments to providers or facilities, 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. Operates computer equipment to complete insurance claims.	5.1 Operates equipment skillfully and efficiently. 5.2 Evaluates condition of equipment and reports need for repair or replacement.
6. Follows employer's policies and procedures.	6.1 Must have punctual work attendance and be dependable.
7. Enhances knowledge and skills to keep up to date.	7.1 Attends continuing education skills activities. 7.2 Obtains current knowledge applicable to state and federal programs as they relate to transmission of insurance claims. 7.3 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.
8. Employs interpersonal expertise to provide good working relationships with patients, employer, employees, and third-party payers.	8.1 Works with employer and employees cooperatively as a team. 8.2 Communicates effectively with patients and third-party payers regarding payment policies and financial obligations. 8.3 Executes job assignments with diligence and skill. 8.4 Assists staff with coding and reimbursement problems. 8.5 Assists other employees when needed. 8.6 Assists with giving fee estimates to patients when necessary.

Fig. 1.2, cont'd.

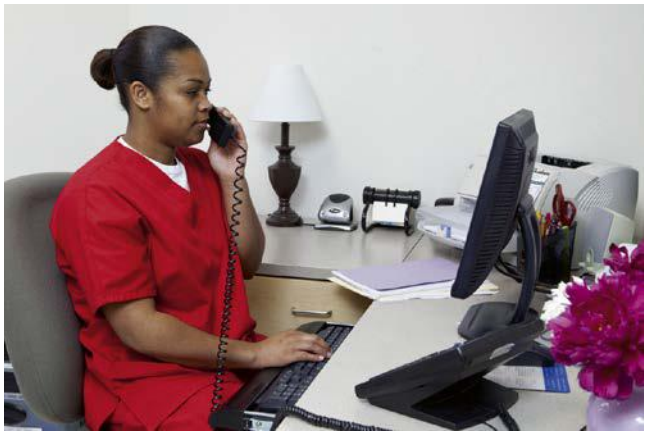


Fig. 1.3 Insurance biller talking to a patient on the telephone about copayment required for an office visit under the patient's insurance plan.

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 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,

MEDICAL INSURANCE SPECIALIST CERTIFICATE PROGRAM

PROGRAM DESCRIPTION: The Medical Insurance program prepares you for employment in the area of medical insurance and health care claims processing. This program also serves the needs of health care personnel interested in upgrading their professional skills. Training in computerized medical billing, CPT-4 and ICD-10-CM coding, and processing medical insurance claims are included in the curriculum. Students may be enrolled on a full-time or part-time basis, and may complete the program by attending either day or evening classes. Accelerated or fast track courses are also available for those wishing to complete this program within a short time period. The program graduates students with marketable skills that are in demand. They are employed in hospitals, insurance companies, private medical laboratories, billing bureaus, and doctors' offices. Graduates may apply credits toward other certificate or associate degree programs.

The following courses are included in this program:

First Semester

Medical Terminology	3 Credits
Administrative Medical Office Management	4 Credits
Biology	3 Credits
Keyboarding	3 Credits
Computer I	2 Credits
	TOTAL 15 Credits

Second Semester

Principles and Applications of Medical Insurance	3 Credits
Current Issues of Medical Insurance	3 Credits
Medical Financial Management	3 Credits
Word Processing	3 Credits
Basic Principles of Composition	3 Credits
	TOTAL 15 Credits

Fig. 1.4 Example of a 1-year medical insurance specialist certificate program offered at a community college. Basic coding is taught as a part of the course in Administrative Medical Office Management and advanced coding is covered in Principles and Applications of Medical Insurance. Biology may be titled Anatomy and Physiology in some colleges. (Reprinted with permission from Community College of Allegheny County, Pittsburgh, PA.)

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, or collectors. 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 so on. Some billers work from their homes and others rent or lease an office.

Flexible Hours

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 vary 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 financial 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.

Inquire at your local vocational rehabilitation center for training disabled individuals.

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. This list is by no means complete; perhaps you can think of additional attributes that might lead to a more successful career.

Skills

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

- Solid foundation and working knowledge of medical terminology, including anatomy, physiology, disease, and treatment terms, as well as the meanings of abbreviations
  Application: Interpretation of patient's chart notes and code manuals.
  Documented Diagnosis: ASHD.
  Locating the diagnostic code using an abbreviation is difficult; therefore, you must be able to translate it. In this case the abbreviation **ASHD** must be translated to arteriosclerotic heart disease.
- Expert use of procedural and diagnostic code books and other related resources
  Application: Code manuals, official coding guidelines, and other reference books are used to assign accurate codes for each case billed.
- Precise reading skills
  Application: Differentiate between the technical descriptions of two different but similar procedures.
  Procedure (CPT) Code No. 43352 Esophagostomy (fistulization of esophagus, external; cervical approach)
  Procedure (CPT) Code No. 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
  Application: Calculate fees and adjustments on the insurance claim forms and enter them into the patient accounts. It is essential that these figures be accurate.
- Knowledge of medicolegal rules and regulations of various insurance programs
  Application: Avoid filing of claims considered fraudulent or abusive because of code selection and program policies. Fraud and abuse will be covered in Chapter 3.
- Knowledge of compliance issues
  Application: Federal privacy, security, and transaction rules in addition to fraud, waste, and abuse.
- Basic keyboarding and computer skills
  Application: Good keyboarding and data entry skills and knowledge of computer programs are essential because the industry increasingly involves practice management software and electronic claims submission.

- Proficiency in accessing information through the internet
  Application: Obtain federal, state, and commercial insurance regulations and current information as needed through the internet. Sign on as a member of a **list service (listserv)**, which is a service run from a website where questions may be posted. Find one composed of working coders to obtain answers on how to code complex, rare, or difficult medical cases.
- Knowledge of billing and collection techniques
  Application: Use latest billing and collection ideas to keep cash flow constant and avoid delinquent accounts.
- Expertise in the legalities of collection on accounts.
  Application: 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
  Application: If you develop your own business as a medical claims and billing specialist, you may be paid according to the amount of paid claims the health care practice is reimbursed. Because you will rely on volume for an income, the more expeditious you become, the more money you earn. Therefore accuracy in selecting the correct codes and data entry and motivation in completing claims also become marketable skills.

Personal Image

To project a professional image, be attentive to apparel and grooming (Fig. 1.5). In a work setting, a uniform may be required, or you might be expected to wear business attire that is conservative and stylish but not trendy. For women, this includes a business suit, dress, or skirt of appropriate length; slacks; sweaters; blouses; and dress shoes. For men, a business suit or dress slacks and jacket, shirt, tie (optional), and dress shoes are appropriate.

Fig. 1.5 Male and female medical personnel who project a clean, fresh, and professional image.

When hired, it is important to discuss appropriate dress code with the supervisor. Keep in mind that fragrances can be offensive or cause allergies to some clients and patients; therefore use good judgment. Fingernails should be carefully manicured and appropriate to the dress code. For women, subdued eye makeup is appropriate for day use. Consult the employer for the office policy regarding body piercings and tattoos.

Remember that you are in a professional environment and must present yourself in such a way.

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 helping you reach the goal of processing the billing and obtaining maximum reimbursement for the patient and physician. Communicate effectively. Be honest, dependable, and on time. Never take part in office gossip or politics. Be willing to do the job and be efficient in how you carry it out.

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. 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. If you work in an office in which patients go by your desk, acknowledge them 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 you 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 your 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 who

enter your office or come to your desk by saying, "I'll be with you in a moment."
3. Identify yourself to callers and people you call.
4. Do not use first names until you know it is appropriate to do so.
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.

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, you may be composing, forwarding, and responding via e-mail with staff in other locations, with patients, and with insurance billers (Fig. 1.6). It is important to set some standards to follow when communicating via e-mail. The messages you send are a reflection of your professional image.

EXAMPLE 1.1 Electronic Mail Address

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

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

1. Identify yourself and the reason for the message.
2. Compose the message in a clear and concise manner using good grammar and proper spelling. Make sure it cannot be misconstrued.
3. Include a descriptive subject line. If a reply changes the topic, then change the subject line.
4. Do not put confidential information in an e-mail message (e.g., patient-identifiable information).
5. Encrypt (code) all files about patients and e-mail attachments and limit the size of attachments.
6. Recognize that all e-mail is discoverable in legal proceedings, so be careful with content and choice of words.
7. Do not use all capital letters for more than one word.
8. Insert a blank line between paragraphs.
9. Surround URLs (long web addresses) with angle brackets [ ] to avoid problems occurring at the end of a line because of the word wrap feature.
10. Do not use variable text styles (bold or italic) or text colors.
11. Quote sparingly when automatically quoting the original message in replies. Some programs allow you to select some text in the original message by pressing a keyboard shortcut, and only that text will be quoted in the reply. Quotation marks should be inserted to differentiate original and new text.
12. Avoid sending or forwarding junk messages (e.g., welcome messages, congratulation messages, jokes, chain messages).
13. Avoid "emoticons," a short sequence of keyboard letters and symbols used to convey emotion, gestures, or expressions (e.g., "smiley" [(; :–)]).
14. Do not respond immediately if a person's e-mail makes you angry or emotional. Put the message aside until the next day and then answer it diplomatically.

Address ➔	To: apcmonitor@shore.net
Subject Line ➔	Subj: **anesthesia modifiers**
Date ➔	Date: Thursday, April 7, 2016
Sender Address ➔	From: brownm@aol.com
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 ➔	Smith Medical Center
E-mail address ➔	brownm@aol.com
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. 1.6 Electronic mail message sent to *APC's Weekly Monitor* asking a question about the use of modifiers.

15. Do not write anything that is racially or sexually offensive.
16. Insert a short signature at the end of the message that includes your name, affiliation, and e-mail and/or URL address.

PROFESSIONAL ETHICS

Ethics are not laws but standards of conduct generally accepted as moral guides for behavior by which an insurance billing or coding specialist may determine the propriety of his or her conduct in a relationship with patients, the physician, co-workers, the government, and insurance companies. You are entrusted with holding patients' medical information in confidence, collecting money for your health care organization, and being a reliable resource for your 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 B.C. and is called the *Code of Hammurabi.* Then, about the fifth century B.C., 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 not only to patients, but also 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.
II. A physician shall deal honestly with patients and colleagues, and strive to expose those physicians deficient in character or competence, or who engage in fraud or deception.
III. A physician shall respect the law and also recognize a responsibility to seek changes in those requirements that 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 within the constraints of the law.
V. A physician shall continue to study, apply, and advance scientific knowledge; 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 services.
VII. A physician shall recognize a responsibility to participate in activities contributing to an improved community.

It is the insurance billing specialist's responsibility to inform administration or his or her 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 your supervisor if you discover that a patient may have questionable issues of care, conduct, or treatment with your 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.

Anyone who uses the internet for health-related reasons has a right to expect that organizations that provide health products, services, or information online will uphold ethical principles. The Internet Healthcare Coalition has developed an eHealth Code of Ethics, which is available at its website (www.ihealthcoalition.org).

It is *illegal* to report incorrect information to government-funded programs, such as Medicare, Medicaid, and TRICARE. 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 (Fig. 1.7).

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.

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

STANDARDS OF ETHICAL CODING

Coding professionals should:

1. Apply accurate, complete, and consistent coding practices for the production of high-quality healthcare data.
2. Report all healthcare data elements (e.g. diagnosis and procedure codes, present on admission indicator, discharge status) required for external reporting purposes (e.g. reimbursement and other administrative uses, population health, quality and patient safety measurement, and research) completely and accurately, in accordance with regulatory and documentation standards and requirements and applicable official coding conventions, rules, and guidelines.
3. Assign and report only the codes and data that are clearly and consistently supported by health record documentation in accordance with applicable code set and abstraction conventions, rules, and guidelines.
4. Query provider (physician or other qualified healthcare practitioner) for clarification and additional documentation prior to code assignment when there is conflicting, incomplete, or ambiguous information in the health record regarding a significant reportable condition or procedure or other reportable data element dependent on health record documentation (e.g. present on admission indicator).
5. Refuse to change reported codes or the narratives of codes so that meanings are misrepresented.
6. Refuse to participate in or support coding or documentation practices intended to inappropriately increase payment, qualify for insurance policy coverage, or skew data by means that do not comply with federal and state statutes, regulations and official rules and guidelines.
7. Facilitate interdisciplinary collaboration in situations supporting proper coding practices.
8. Advance coding knowledge and practice through continuing education.
9. Refuse to participate in or conceal unethical coding or abstraction practices or procedures.
10. Protect the confidentiality of the health record at all times and refuse to access protected health information not required for coding-related activities (examples of coding-related activities include completion of code assignment, other health record data abstraction, coding audits, and educational purposes).
11. Demonstrate behavior that reflects integrity, shows a commitment to ethical and legal coding practices, and fosters trust in professional activities.

Fig. 1.7 American Health Information Management Association (AHIMA) Codes of Ethics, revised and adopted by AHIMA House of Delegates, 2008. (Copyright © 2008 American Health Information Management Association. All rights reserved.)

ancillary service providers. The health care organization you are employed by 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 his or her employer to determine whether he or she is 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. If you knowingly submit a false claim or allow such a claim to be submitted, you can be liable for a civil violation. If you conceal information or fail to disclose it to obtain payment, you can be held liable. If you are not the person preparing a false claim, but you mail or electronically file it, you can be implicated in mail or wire fraud.

If any staff member within a health care organization, or any provider of services asks you as the insurance biller to do something that is the least bit questionable, such as writing off patient balances for certain patients automatically, contact your supervisor and make sure you have a legal document or signed waiver of liability relieving you of the responsibility for such actions. If you notice a problem, it is your responsibility to correct it and to document your 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 or coder. 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. Always check in your state 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 his or her 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 your state's department of insurance and insurance commissioner to determine whether you should be licensed.

FUTURE CHALLENGES

As you begin your study to become an insurance billing specialist, remember that you are expected to profitably manage a health care organization's financial affairs or patient accounts; otherwise, you will not be considered qualified for this position. In subsequent chapters, you will learn the valuable information and skills necessary to help you achieve this goal. You will be expected to do the following:

- Know billing regulations for each insurance program and managed care plan 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. Train so that you become familiar with other aspects of the health care organization.
- Discover opportunities to advance your career.
- 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 towards and the professional organizations that offer certification.

KEY POINTS

This is a brief chapter review, or summary, 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 book, which appears in a section before the index.

1. 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.
2. Individuals who help patients organize and file claims are called *CAPs*.
3. 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.
4. 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 his or her own billing service. In this career, jobs can be rewarding for persons with disabilities.
5. 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.
6. Becoming a professional is a gradual process and one must project an appropriate image and develop as a courteous and respectful team player.
7. Etiquette in a medical setting must be adhered to routinely and one must behave ethically at all times.
8. 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.*
9. 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.
- Answer the fill-in-the-blank, multiple-choice, and true/false questions in the *Workbook* to reinforce the theory learned in this chapter and help prepare for a future test.
- Complete the assignments in the *Workbook* to help develop critical thinking and writing skills. As you proceed through the assignments in the *Workbook,* you will broaden your knowledge of medical terminology and gain an entry-level skill in diagnostic and procedural coding and insurance claim completion.
- 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. Identify the difference between disclosure and use of PHI and discuss exceptions to HIPAA.
7. Illustrate the difference between privileged and nonprivileged information.
8. Explain patient rights under HIPAA.
9. Explain responsibilities of the health care organization to protect patient rights under HIPAA.
10. State the guidelines for HIPAA privacy compliance.
11. List the three major categories of security safeguards under HIPAA.
12. Discuss the Security Rule and how it relates to coding and billing.
13. Define the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).
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.
17. Discuss what to expect from a health care organization when it comes to various HIPAA policies and procedures.

KEY TERMS

American Recovery and Reinvestment Act
authorization
authorization form
breach of confidential communication
business associate
clearinghouse
confidential communication
confidentiality
consent
covered entity
designated record sets
disclosure
electronic media
health care organization
The Health Information Technology for Economic and Clinical Health 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
Patient Protection and Affordable Care Act of 2010
portability
preexisting condition
privacy
privacy officer, privacy official
privileged information
protected health information
psychotherapy notes
security officer
Security Rule
transaction
use

KEY ABBREVIATIONS

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

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, Public Law 104-191. 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 HIPAA legislation projected long-term benefits that include the following:

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

Title I: Health Insurance Reform

The primary purpose of HIPAA *Title I: Health Insurance Reform* is to provide continuous insurance coverage for workers and their dependents when they change or lose jobs. This aspect of HIPAA affects individuals as consumers. 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 poor health, 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 important to understand, too, 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 the health care practice setting and aims to reduce administrative costs and burdens. Standardizing electronic transmissions of billing and payment information reduces the number of forms and methods used in the claims processing cycle. 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 (Administrative Simplification) that will directly pertain to your work in a health care organization:

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

These main parts will be discussed in detail in this chapter.

Defining HIPAA Roles, Relationships, and Key Terms

Department of Health and Human Services

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. When speaking about HIPAA, *Secretary* refers to the DHHS Secretary or any officer or employee of DHHS who has the authority to oversee HIPAA issues.

Office of E-Health Standards and Services

The Office of E-Health Standards and Services is an office of the Centers for Medicare and Medicaid Services (**CMS**). It enforces the insurance portability and transaction and code set requirements for Medicare and Medicaid programs. **Portability** is defined as an employee's right to maintain health care benefits under a group health plan when leaving a job. When this occurs, the former employee has the option to continue his or her group health plan benefits; however, he or she is responsible for the *total* cost of the benefit.

The Office for Civil Rights

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.

Key HIPAA Terms

Electronic media refers to the mode of electronic transmission, including the following:

- Internet (online mode—wide open)
- Extranet or private network using internet technology to link business parties
- Leased telephone or dial-up telephone lines, including fax modems (speaking over the telephone is not considered an electronic transmission)
- Transmissions that are physically moved from one location to another using removable or digital memory medium such as magnetic tape or disk, optical disk, or digital memory card

Electronic forms of media can include optical disk (compact disk [CD] or DVD), USB flash drive, or file transfer protocol (**FTP**) over the internet. Voice-over-modem faxes, which use a telephone line, are not considered electronic media, although a fax from a computer (for example, using the WinFax program) is considered an electronic medium.

A ***transaction*** refers to the transmission of information between two parties to carry out financial or administrative activities related to health care. These data transmissions include information that completes the insurance claim process and are discussed later in the text.

Under HIPAA, the term ***covered entity*** applies to any health care provider, health care organization, health plan, or clearinghouse that transmits health information in electronic form for any number of transactions.

HIPAA's definition of a **health care organization** extends to anyone who provides health care services to a patient. In addition to physicians, this includes hospitals, ambulance service providers, clinics, physician's assistants, nurse practitioners, social workers, chiropractors, dentists, 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 office, 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)** to develop and implement the covered entities' policies and procedures (**P&P**). The organization's PO may hold another position within the health care organization or may not be an employee of the organization at all. Sometimes the PO is a contracted professional who is available to the health care organization in an advisory capacity or interim compliance officer. This advisory role may be filled by an attorney or other professional with extensive compliance experience.

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. Covered entities should have a business associate agreement in place with all entities that work with them. These need to specifically outline how the business associate complies with HIPAA legislation. For example, if the health care organization's medical billing is performed by an outside service, the billing service is a business associate of the covered entity (the health care organization). See Boxes 2.1 and 2.2 for additional information on business associates.

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 his or her health information
- Prohibits disclosure that would be allowed under HIPAA
- Narrows the duration of an authorization to release information

For example, under HIPAA, a covered entity is required to provide an individual access to the 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 ten 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 at least within a shorter time frame.

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.

Refer to Box 2.1 for titles of additional HIPAA-related terms.

BOX 2.1 Overseers of HIPAA Functions

A covered entity transmits health information in electronic form in connection with a *transaction* covered by HIPAA. The covered entity may be (1) a health plan carrier, such as Blue Cross/Blue Shield; (2) a health care clearinghouse through which claims are submitted; or (3) a health care organization, such as the primary care physician, hospital, or laboratory.

A business associate is a person who, on behalf of the covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information (IIHI). 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 provider's practice 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).

A health care provider is a person trained and licensed to provide care to a patient and also 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.

Privacy and security officers oversee the HIPAA-related functions. These individuals may or may not be employees of a particular health care practice. A privacy officer or privacy official (PO) is designated to help 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.

A **security officer** protects the computer and networking systems within the practice and implements protocols such as password assignment, backup procedures, firewalls, virus protection, and contingency planning for emergencies.

BOX 2.2 HIPAA Help

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, the health care provider is a covered entity and must comply with HIPAA.

TRANSACTION AND CODE SET REGULATIONS

HIPAA has been part of a great shift in processing electronic data. 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; 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, Ninth Revision, Clinical Modification* (ICD-9-CM), Volumes I to III (replaced in 2016 by ICD-10-CM for diagnostic coding, and ICD-10-PCS for inpatient procedure coding)

- *Current Procedural Terminology* (CPT) for medical procedure coding
- *Healthcare Common Procedure Coding System* (HCPCS) for medical procedures and supply coding
- *Current Dental Terminology* (CDT) for dental procedure coding

HIPAA electronic transaction standards requires all covered entities to use version 5010 ANSI X12. Not only does this ensure that all claims are submitted in the same format, but all payers are then required to communicate payment, denial, and pended claims in the same format as well. These transaction and code set standards created a common language among providers and other health care organizations and payers that increases 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
- Premium payments

NATIONAL IDENTIFIERS

HIPPA 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. While the first two types of identifiers have already been implemented, 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 against it raise concerns over privacy. The purpose of the identifiers is to further standardize electronic transmissions of claim data.

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 used to submit and process health care claims. NPIs are assigned to every provider, group practice, health care facility, pharmacy, and other health care organization. If you submit a claim for a provider in a group practice, both provider's NPI and the group practice's NPI must appear on the claim.

THE PRIVACY RULE: CONFIDENTIALITY AND PROTECTED HEALTH INFORMATION

> *What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about.*
>
> ***Hippocrates, 400 B.C.***

The Hippocratic Oath, federal and state regulations, professional standards, and ethics all address patient privacy. For years, health care organizations locked health records in file cabinets and refused to share patient health information. Patients now have specific rights regarding how their health information is used and disclosed because federal and state laws regulate the protection of an individual's privacy. 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

Current technology allows easy access to health care information. HIPAA imposes new requirements on health care organizations with regards to this. Since computers are essential to the health care organizations, confidential health data is now sent across networks, e-mailed over the internet, and even accessed by hackers. Sometimes few safeguards are taken to protect data and prevent information from being intercepted or lost. 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 certain health care transactions electronically.

Key Terms in the Privacy Rule

Privacy, Confidentiality, and Use

Privacy is the condition of being secluded from the presence or view of others. **Confidentiality** is using discretion in keeping secret information. Integrity plays an important part in the health care setting. Health care workers need a solid understanding of HIPAA's basic requirements. An employee must have strong moral principles and must be committed to protecting the privacy and rights of the practice's patients.

Health care organizations and their staff use and disclose health information on a regular basis. Records are also shared between providers in the course of patient care. Information is released to health plans to process claims. ***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.

Protected Health Information

Protected health information (PHI) is any information that identifies an individual and describes his or her health

EXAMPLE 2.1 Protected Health Information in a Health Care Organization

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

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 in electronic form or transmitted, or maintained 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 health care organization's computerized practice management and billing system, spoken words, and x-ray films.

Disclosures, 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**).

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 giving information about a patient you are scheduling for a procedure to the health care facility's outpatient surgery center. See Table 2.1 for examples of uses and disclosures of PHI.

Consent is the verbal or written agreement that gives approval to some action, situation, or statement. In health care, 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 Figs. 2.1 to 2.2 for an example of a consent for release of information form.

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 Rule. Authorization is an individual's formal, written permission to use or disclose his or her personally identifiable health information for purposes other than TPO. For example, if you change primary care providers, you will need to sign an authorization to have your health records sent to your 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 Box 2.3, which details the regulations for disclosing the minimum necessary PHI, de-identification of PHI, marketing related to the patient, and fundraising activities related to patients. See Fig. 2.3 for an example of an authorization for release of information.

Individually Identifiable Health Information

Individually identifiable health information (IIHI) is any part of an individual's health information, including demographic information (for example, address or date of birth), 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 you as a health care provider are talking to an insurance representative, you 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. 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 your town who is indigent and has stomach problems, the staff member is not divulging information that would identify the patient.

Designated Record Set

HIPAA gives an individual the right to access his or her 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 designated record set is one that contains information used to make decisions about a patient. A covered entity is not required to provide explanatory notes or create new information in the record set. 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.

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

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

Permitted Disclosures (No Authorization Required)	What It Means for Your 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 his or her 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 your 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	You 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 Your Health Care Organization**
Disclose PHI to persons involved with the patient	You 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 Your 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	You 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	You 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	You 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 your health care practice does fundraising or marketing, you 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.

to do their job. It should only be shared on a need-to-know basis. For example, a coding specialist will need access to the entire patient's health record to code a visit. However, the receptionist for a medical office will most likely not need to see the entire record to schedule an appointment for a patient. The Minimum Necessary Rule applies to business associates as well. If a physician is referring a patient to a prosthetic manufacturer (business associate), 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.

Privileged and Nonprivileged Information

When working with health records, all health care staff members are responsible for maintaining the confidentiality of patients' health information. Example 2.1 lists some of the PHI that is typical in a health care organization and that falls under HIPAA compliance regulations.

The patient record and any photographs obtained are confidential documents and require an authorization form signed by the patient to release information (see Figs. 2.1 to 2.4). If the form is a photocopy, it is necessary to state that the patient approves the photocopy or write to the patient and obtain an original signed document.

RELEASE OF MEDICAL INFORMATION

PATIENT INFORMATION

Patient Name _____

Address _____ Social Security # _____

City _____ State _____ ZIP _____ Birth date ____/____/____

Phone (Home) _____ Work _____

RELEASE FROM:

Name _____

Address _____

City _____ State _____ ZIP _____

RELEASE TO:

Name _____

Address _____

City _____ State _____ ZIP _____

INFORMATION TO BE RELEASED:

1. GENERAL RELEASE:

___Entire Medical Record (excluding protected information)
___Hospital Records only (specify)_____
___Lab Results only (specify) _____
___X-ray Reports only (specify) _____
___Other Records (specify) _____

2. INFORMATION PROTECTED BY STATE/FEDERAL LAW:
If indicated below, I hereby authorize the disclosure and release of information regarding:

___Drug Abuse Diagnosis/Treatment
___Alcoholism Diagnosis/Treatment
___Mental Health Diagnosis/Treatment
___Sexually Transmitted Disease

PATIENT AUTHORIZATION TO RELEASE INFORMATION:

Authorization is valid for 60 days only from the date of my signature. I reserve the right to revoke this authorization at any time prior to 60 days (except for action that has already been taken) by notifying the medical office in writing.

I understand that my records are protected under HIPAA (Health Insurance Portability and Accountability Act) Standards for Privacy of Individually Identifiable Information (45 CFR Parts 160 and 164) unless otherwise permitted by federal law. Any information released or received shall not be further relayed to any other facility or person without my written authorization. I also understand that such information will not be given, sold, transferred, or in any way relayed to any other person or party not specified above without my further written authorization.

I hereby grant authorization to release the information listed above. I certify that this request has been made voluntarily and that the information given above is accurate to the best of my knowledge.

_____ _____
Signature of Patient/Legally Responsible Party **Date**

_____ _____
Witness Signature **Date**

Fig. 2.1 Consent for release of information form. (Modified from Bonewit-West, K., Hunt, S., & Applegate, E. (2013). *Today's medical assistant: Clinical & administrative procedures* (2nd ed.). St. Louis: Saunders.)

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 you see, hear, or read 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. 2.5). Such agreements should be updated periodically to address issues raised by the use of new technologies.

Privileged 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. Some states have passed laws allowing certain test results (for example, disclosure of the presence of the human immunodeficiency virus [HIV] or alcohol or substance abuse) and other information to be placed separate from the patient's health record. Some states require a special authorization form is used to release this information.

Nonprivileged Information

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. An attending physician may require complete access to the health record because the information may have some effect on the treatment of the patient. An x-ray technician would not necessarily need to know everything in the record.

Exceptions to HIPAA

Unauthorized release of information is called **breach of confidential communication** and is considered a HIPAA violation. Violations may lead to substantial fines.

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 HIPAA, but you may find that some health care organizations use it. (From Fordney, M. T., French, L. (2003). *Medical insurance billing and coding: a worktext.* Philadelphia: Elsevier.)

Confidentiality between the physician and patient is automatically waived in the following situations:

1. 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. Other managed care providers need to know about the patients if they are involved in the care and treatment of members of the MCO.
2. 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.
3. 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.
4. 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.

BOX 2.3 HIPAA Help

These key terms are addressed in the Notice of Privacy Practices (NPP) that applies to the patient's right to request restrictions on certain uses and disclosures of protected health information (PHI).

- **Minimum necessary.** Privacy regulations require that use or disclosure of only the minimum amount of information necessary to fulfill the intended purpose be permitted. There are some exceptions to this rule. You do not need to limit PHI for disclosures to health care organizations for treatment, the patient, DHHS for investigations of compliance with HIPAA, or as required by law. 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 clinical and billing records. Simple procedure and policy (P&P) about appropriate access to PHI may be sufficient to satisfy the Minimum Necessary requirement. 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. Remain knowledgeable about your office's policy regarding Minimum Necessary. If you are strictly scheduling appointments, you may not need access to the clinical record. An x-ray technician will most likely not need to access the patient billing records. 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, you may implement policies and procedures, or standard protocols, for what will be disclosed. These disclosures would be common in your practice. 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.

  As a general rule, remember that you must limit your requests to access PHI to the Minimum Necessary to accomplish the task for which you will need the information.
- **De-identification of confidential information.** Other requirements relating to uses and disclosures of PHI include health 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 individually identifiable health information (IIHI). Most health care organizations will never need to de-identify patient information and the requirements for de-identifying PHI are lengthy. 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.
- **Marketing.** When communicating about a product or service, the goal is to encourage patients to purchase or use the product or service. For example, a dermatologist may advertise for a discount on facial cream when you schedule a dermabrasion treatment. You will not likely be involved in marketing but keep in mind the general rule that PHI (including names and addresses) cannot be used for marketing purposes without the specific authorization of the patient. Sending appointment reminders and general news updates about your organization and the services you provide is not considered marketing and does not require patient authorization.
- **Fundraising.** Again, you will likely not be involved in fundraising activities but HIPAA allows demographic information and dates of care to be used for fundraising purposes without patient authorization. The disclosure of any additional information requires patient authorization. Your organization's Notice of Privacy Practices will state that patients may receive fundraising materials and are given the opportunity to opt out of receiving future solicitations.

5. 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.
6. When there is a suspicious death or suspected crime victim, health care organizations must report cases to proper law enforcement authorities.
7. When the physician 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.
8. 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.

Patients' Rights

Right to Privacy

All patients have a right to privacy. It is important never to discuss patient information other than with the physician, an insurance company, or an individual who has been authorized by the patient.

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. If confidential documents are on your desk, patients can easily see them as they walk by. Either turn the documents over or lock them in a secure drawer when you leave your desk, even if you are gone for only a few moments.

Don't: Leave a computer screen with patient information visible, even for a moment, if another patient may see the data. If patient information is on your computer, either turn the screen off or save it on disk, lock the disk in a secure place, and clear the information from the screen.

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.

REQUIRED ELEMENTS OF HIPAA AUTHORIZATION

Identification of person (or class) authorized to request

Identification of person (or class) to whom covered entity is to use/disclose

Description of information to be released with specificity to allow entity to know which information the authorization references

Description of each purpose of the requested use or disclosure

Expiration date, time period, or event

Statement that is revocable by written request

Individual's (patient's) signature and date

Statement of representative's authority

Authorization for Release of Information

PATIENT NAME: Levy (LAST) Chloe (FIRST) E. (MI) (MAIDEN OR OTHER NAME)
DATE OF BIRTH: 02 (MO) - 12 (DAY) - 1950 (YR) SS# 320 - 21 - 3408 MEDICAL RECORD #: 3075
ADDRESS: 3298 East Main Street CITY: Woodland Hills STATE: XY ZIP: 12345-0001
DAY PHONE: 013-340-9800 EVENING PHONE: 013-549-8708

I hereby authorize Gerald Practon, MD **(Print Name of Provider) to release information from my medical record as indicated below to:**
NAME: Margaret L. Lee, MD
ADDRESS: 328 Seward Street CITY: Anytown STATE: XY ZIP: 45601-0731
PHONE: 013-219-7698 FAX: 013-290-9877

INFORMATION TO BE RELEASED:

	DATES:
☒ History and physical exam	6-8-20XX
❑ Progress notes	
❑ Lab reports	
❑ X-ray reports	
❑ Other:	

I specifically authorize the release of information relating to:
❑ Substance abuse (including alcohol/drug abuse)
❑ Mental health (including psychotherapy notes)
❑ HIV related information (AIDS related testing)
X
SIGNATURE OF PATIENT OR LEGAL GUARDIAN DATE

PURPOSE OF DISCLOSURE: ❑ Changing physicians ☒ Consultation/second opinion ❑ Continuing care
❑ Legal ❑ School ❑ Insurance ❑ Workers Compensation
❑ Other (please specify):

1. I understand that this authorization will expire on 09/01/20XX (Print the Date this Form Expires) days after I have signed the form.
2. I understand that I may revoke this authorization at any time by notifying the providing organization in writing, and it will be effective on the date notified except to the extent action has already been taken in reliance upon it.
3. I understand that information used or disclosed pursuant to this authorization may be subject to redisclosure by the recipient and no longer be protected by Federal privacy regulations.
4. I understand that if I am being requested to release this information by Gerald Practon, MD (Print Name of Provider) for the purpose of:
   a. By authorizing this release of information, my health care and payment for my health care will not be affected if I do not sign this form.
   b. I understand I may see and copy the information described on this form if I ask for it, and that I will get a copy of this form after I sign it.
   c. I have been informed that Gerald Practon, MD (Print Name of Provider) will/will not receive financial or in-kind compensation in exchange for using or disclosing the health information described above.
5. I understand that in compliance with XY (Print the State Whose Laws Govern the Provider) statute, I will pay a fee of $ 5.00 (Print the Fee Charged). There is no charge for medical records if copies are sent to facilities for ongoing care or follow up treatment.

Chloe E. Levy 6/1/XX OR
SIGNATURE OF PATIENT DATE PARENT/LEGAL GUARDIAN/AUTHORIZED PERSON DATE

RECORDS RECEIVED BY DATE RELATIONSHIP TO PATIENT

FOR OFFICE USE ONLY
DATE REQUEST FILLED BY:
IDENTIFICATION PRESENTED FEE COLLECTED $

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 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 physician'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.)

Fig. 2.4 Patient signing a consent form.

Fig. 2.5 Insurance billing specialist consulting with the supervisor or office manager about office policies regarding release of a patient's health record.

- Ask the patient to fax a sheet with his or her 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 physician 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 (Fig. 2.5).

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

Privacy Rules: Patient Rights 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:

1. *Right to **Notice of Privacy Practices (NPP),*** a document in plain language that is usually given to the patient at the first visit or at enrollment. 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 entities 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

2. *Right to request restrictions on certain uses and disclosures of PHI.* Patients have the right to ask for restrictions on how a health care organization uses and discloses PHI for TPO. 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.
3. *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 practice's compliance endeavors.
4. *Right to access (inspect and obtain a copy of) PHI.* 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.

BOX 2.4 HIPAA Help

According to the HIPAA Privacy Rule, the term *psychotherapy notes* means notes that are recorded in any medium by a mental health professional. These document or analyze the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's health record. Under this rule, a health care professional is not obligated to disclose these notes to third party payers or even to the patient. Some information, such as prescriptions, session start and end times, treatment modalities, and any summary of diagnosis or prognosis, are not considered to be part of the psychotherapy notes. To be safeguarded, psychotherapy notes must be kept separate from the patient's health record.

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 his or her 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 (Box 2.4)
- 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 him- or herself 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.

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.

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

In general, psychotherapy notes are defined as the information that is the recorded (in any manner) documentation and/or analysis of conversation. 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 (for example, what occurred and how she felt) is considered the psychotherapy notes and cannot be released without Jane Doe's specific permission.

It is also important to understand that patients do not have the right to obtain a copy of psychotherapy notes under HIPAA (see Box 2.4). 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 earlier.

5. *Right to request an amendment of PHI.* 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 physician.
   - 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.
6. *Right to receive an accounting of disclosure of PHI.* 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. Additional accountings may be assessed a cost-based fee (Boxes 2.5 and 2.6). 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,

BOX 2.5 HIPAA 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 you become acclimated to your organization's policies and procedures regarding the handling of protected health information (PHI), you will be better able to recognize that your position plays an important part in HIPAA compliance.

BOX 2.6 HIPAA Help

Health care organizations and staff are not likely to read the *Federal Register* from cover to cover. However, it is important that you are familiar with it. The *Federal Register* is a daily newspaper published by the National Archives and Records Administration. It contains federal regulations, proposed rules, and other important documents. New legislation that affects the health care world will always appear in this publication.

You should be familiar with the general forms used in your practice setting. 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 practice. Health care staff must learn about the particular "authorization" forms used in their office. Psychotherapy notes are handled separately under HIPAA. Such notes have additional protection, specifically that an authorization for any use or disclosure of psychotherapy notes must be obtained.

Your organization will be expected to handle requests made by patients to exercise their rights. You must know your office's process for dealing with each specific request. With your understanding of HIPAA and your organization's policy manual, you will be guided in procedures specific to your health care organization.

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.

Verification of Identity and Authority

Remember, before any disclosure, you must verify the identity of persons requesting PHI if they are unknown to you. You may request identifying information, such as date of birth, Social Security number, or even a code word stored in your practice management 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.

You must also verify that the requestor has the right to receive the PHI and identify the need for the PHI. Exercising professional judgment fulfills your verification requirements for most disclosures because you are 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 on your part with respect to HIPAA.

Validating Patient Permission

Before making any uses or disclosures of confidential health information other than for the purposes of TPO, your office must have appropriate patient permission. Always check for conflicts between various permissions your office may have on file for a given patient. This information should be maintained either in your practice management system or in the health record, where it can be easily identified and retrieved.

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 physician, this would be a conflict. In general, the more restrictive permission would take precedence. Privacy regulations allow resolving conflicting permissions either by obtaining 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.

Obligations of the Health Care Organization

Training

Under HIPAA regulations, a covered entity must train all members of its staff. This training must include the practice's P&P with respect to PHI as it pertains to their function within the organization. This training will address how each employee's role relates to PHI in his or her office or department. HIPAA training focuses on how to handle confidential information securely in the health care setting. Training should be completed as part of a new hire orientation and then annually. All training must be documented.

Safeguards: Ensuring That Confidential Information Is Secure

Every covered entity must have appropriate safeguards to ensure the protection of an individual's confidential health information. Such safeguards include administrative, technical, and physical measures that will reasonably safeguard PHI from

BOX 2.7 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.

any use or disclosure that violates HIPAA, whether intentional or unintentional (Box 2.7). Examples of security safeguards are discussed later in this chapter.

Complaints to Health Care Practice and Workforce Sanctions

Individuals, both patients and staff, must be provided with a process to make a complaint concerning the P&P of the covered entity. If a violation involves the misuse of PHI, this incident should be reported to the organization's PO. Should there be further cause, the OCR also may be contacted.

Staff members are subject to appropriate sanctions for failure to comply with the P&P regarding PHI set forth in the organization. The types of sanctions applied vary, depending on the violation and its mitigating factors. Sanctions can range from a warning to suspension to termination. This information should be covered in the policy and procedures manual. Written documentation of complaints and sanctions must be kept on file.

Mitigation

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 breaches. 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 you learn that you 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 practice's business associates. Being proactive and responsible by mitigating reduces the potential for a more disastrous outcome from the breach or violation.

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 the following:

- Individuals, for exercising HIPAA privacy rights
- Individuals, for filing a complaint with DHHS; for testifying, assisting, or participating in an investigation about the covered entity's privacy practices; or for reasonably opposing any practice prohibited by the regulation

THE SECURITY RULE: ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS

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. Security measures encompass all administrative, physical, and technical safeguards in an information system. The Security Rule addresses only ePHI, but the concept of preserving PHI that will become ePHI makes attention to security for the entire office 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.

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

- Information access controls authorize each employee's physical access to ePHI. This is management of passwords for each individual employee. 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 located on the computer. Each user should have a unique user name and an unshared, undisclosed password to log in to any computer with access to PHI. Identifying each unique user allows the functions of auditing and access controls to be 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 practice management system and the paper records or charges.
- 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 are technologic controls that are put in place to protect and control access to information on computers in 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 log-ins to the computer system, administrative activity, and changes to data. This includes changing passwords, deleting user accounts, and creating new user accounts.
- Automatic log-offs 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 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 disks 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

Computer Confidentiality

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. 2.6). 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.

Prevention Measures

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 disks or tapes 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. Check and double check the credentials of any consultant hired.
5. Read the manuals for the equipment, especially the sections titled "Security Controls," and follow all directions.
6. Store confidential data on disks rather than only on the computer's hard drive. Disks 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. 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.
8. A strong password:
   - Is at least eight characters long.
   - Does not contain your user name, 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.
     - Example: Iluv2pla2BA4$
9. 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.

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

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

American Recovery and Reinvestment Act (ARRA) of 2009 signed into law by President Obama. ARRA contained incentives for adopting health care information technology that are designed to speed up the adoption of electronic health record systems for many health care organizations. Because this legislation promoted a massive expansion in the exchange of ePHI, the purpose of the HITECH Act was to strengthen the HIPAA privacy protections and rights. 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 very 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 brought greater responsibility to the business associate. It requires all business associates to comply with the HIPAA Security Rule by February 17, 2010, 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.

Under the HITECH Act, if a breach were to occur, the HITECH Act requires a covered entity to notify the affected party directly without delay. In no case should notification be later than 60 calendar days after the discovery of a breach. Enforcement of the notification of breach began on February 22, 2010.

The standard for reporting breaches was modified in 2013 under the HIPAA Omnibus Rule. 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. This is based on a risk assessment of certain factors or unless the breach fits within certain exceptions. Health care organizations must develop policies that apply to these standards.

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.

In health care, all files and electronic data must be encrypted and destroyed when the records no longer need to be retained. 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 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.

Increased 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 are 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

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 care organization refuses to give patients copies of their records when requested. In this case, OCR may apply the penalty per day that the practice was in violation, or 365 days for an entire year.

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

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 was effective March 26, 2013. The rule enhances patients' privacy rights and protections, especially regarding genetic information. It strengthens the OCR's ability to enforce the HIPAA privacy and security protections in the face of the expanded use of electronic health records. The new rule also expands many of the requirements of business associates who receive PHI and their subcontractors, holding them to the same standards of covered entities. As mentioned earlier, the Omnibus Rule also clarifies when breaches of unsecured health information must be reported to DHHS. The rule streamlines the authorization process. It increases the restrictions on use of PHI in research and marketing and raises the penalties for negligent disclosures.

The new rule requires covered entities to update policies applicable to deceased persons. It states that a covered entity may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person and determining the cause of death.

The Omnibus Rule strengthens the need for timeliness in response to a patient's request for records. It also adds a provision permitting providers to disclose proof of a child's immunization records to schools if the school is required by law to have such proof. The rule also makes it easier for parents and others to disclose the child's immunization records by giving them the ability to authorize the disclosure through oral consent.

Consequences of Noncompliance With HIPAA and the HITECH Act

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.

Since the 2003 HIPAA Privacy Rule compliance date, the OCR has investigated more than 160,000 complaints. 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.

DHHS announced its first enforcement action resulting from a violation of the HITECH Act Breach Notification Rule in 2012, which placed a monetary settlement of $1.5 million per breach on the accused. This enforcement action sent a clear message to the health care community that the OCR expects health care organizations to have a carefully designed and active HIPAA compliance plan in place.

More recent settlements have brought millions of dollars in restitution. In May 2017, HHS announced that St. Luke's–Roosevelt Hospital Center, Inc. paid $387,200.00 to settle violations. Allegedly, staff disclosed PHI revealing sensitive information about HIV to a patient's employer. During the investigation, the OCR learned that the same hospital had a similar breach 9 months earlier and had not addressed the weak areas in their P&P to ensure it would not happen again.

In the same month, Memorial Hermann Health System agreed to pay $2.4 million to HHS and to follow a corrective action plan to settle their violations. In 2015 a patient had presented to the facility with a fraudulent identification card. Staff alerted the appropriate law enforcement authorities and the patient was arrested. This was a permissible disclosure.

Fig. 2.7 HIPAA, privacy, and security affect every level of the health care organization. (From iStock photo.com)

However, the health care organization went on to issue a press release containing the patient's name in the title. The corrective action plan requires Memorial Hermann Health System to update their P&P and to train their staff.

Again, 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 115,143 individuals where some employees had inappropriately disclosed the information to other office staff. A former employee's login credentials had been used for a year to access more than 80,000 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).

APPLICATION TO THE HEALTH CARE SETTING

HIPAA affects all areas of the health care office, from the reception area to the provider (see Fig. 2.7). 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.

Reasonable safeguards are measurable solutions based on accepted standards that are implemented and periodically monitored to demonstrate that the office is in compliance. Reasonable efforts must be made to limit the use or disclosure of PHI. If you are the front desk receptionist and you close the privacy glass

between your 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 you are in the reception area and you close the privacy glass before having a confidential conversation but are still overheard by an individual in the waiting room, this would be incidental. You have applied a reasonable safeguard to prevent your conversation from being overheard. The OCR has addressed what is permissible with regard to incidental disclosures. Examples follow.

1. As discussed earlier in this chapter, use caution when handling patient and insurance inquiries over the phone or via e-mail. Ensure that the person you are releasing information to has the right to receive it.
2. Health care professionals may discuss laboratory test results with a patient or other provider in a joint treatment area. A health care professional is an individual who has been trained in a health-related field, whether clinical or administrative. The professional may be licensed, certified, or registered by a state or government agency or professional organization.
3. A physician may discuss a patient's condition or plan of care in the patient's treatment area or hospital room.
4. A pharmacist may discuss a prescription with a patient over the pharmacy counter or with a physician or the patient by telephone.
5. A physician may give instructions to a staff member to bill a patient for a certain procedure even if other individuals in the reception room can overhear the conversation.
6. 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.

Organization and Staff Responsibilities in Protecting Patient Rights

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.

Health care organizations face challenges in applying the HIPAA requirements; do not let these overwhelm you. Appropriate steps are required to build protections specific to your health care organization. Compliance is an ongoing effort involving teamwork. Understand your office's established P&P. Monitor your own activities to ensure that you are following the required procedures. Do not take shortcuts when your actions involve patient privacy and security.

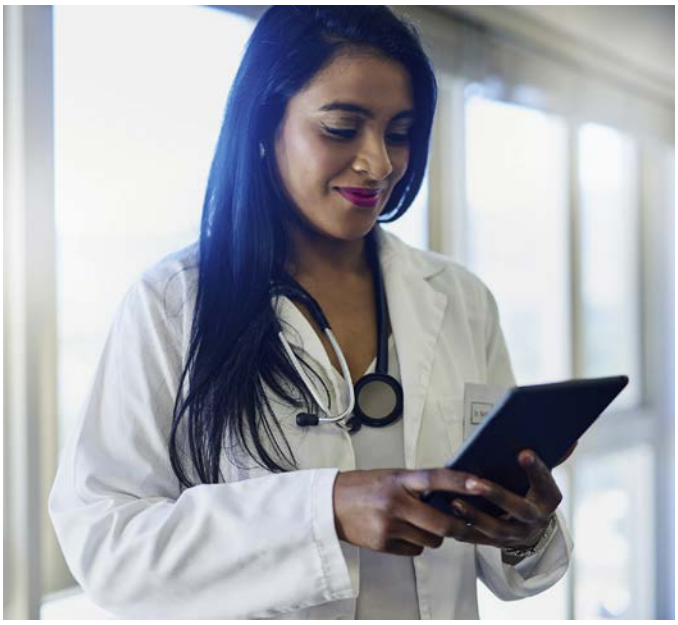


Fig. 2.8 Privacy and security must be considered in every aspect of your job, from phone conversations to computer use to physical surroundings. (From iStock photo.com)

BEST PRACTICES TO AVOID COMMON HIPAA VIOLATIONS

As an insurance billing specialist, you will likely answer the telephone and speak during the course of your business, and there may be uncertainties about what questions you can and cannot answer. Reasonable and appropriate safeguards must be taken to ensure that all confidential health information in your office is protected from unauthorized and inappropriate access, in both verbal and written forms (Fig. 2.8).

- 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 your computer system 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.