KEY TERMS

abuse
ANSI ASC X12N 837
authorization
black box edit
breach of confidentiality
business associate
carrier
case law
check digit
civil law
clearinghouse
Clinical Data Abstraction Centers (CDACs)
code pairs (edit pairs)
common law
confidentiality
consent
contract
criminal law
Current Dental Terminology (CDT)
deposition
direct treatment provider
electronic transaction standards
encrypted
Federal Claims Collection Act of 1966
Federal False Claims Act
Federal Register
first party
fiscal intermediary (FI)
flat file
fraud
guardian(s)
interrogatory
listserv
Medicare Bulletin
minimum data
modifier
National Drug Code (NDC)
National Health PlanID (PlanID)
National Individual Identifier
National Provider Identifier (NPI)
National Standard Employer Identifier Number (EIN)
National Standard Format (NSF)
overpayment
Payment Error Prevention Program (PEPP)
payment error rate
precedent
privacy
Privacy Act of 1974
Privacy Rule
qui tam
regulation
second party
security
Stark II regulations
statute
statutory law
subpoena
subpoena duces tecum
third party
UB-92
upcoding
verbal contract

Chapter 5 Legal and Regulatory Considerations

OBJECTIVES

Upon successful completion of this chapter, you should be able to:

1. Define key terms.
2. Provide examples of a statute, regulation, and case law.
3. Explain the use of the *Federal Register*.
4. Discuss ways the insurance specialist can obtain information about new laws and regulations.
5. Give examples of breaches of confidentiality.
6. State the importance of obtaining the patient's signature for the "Authorization for Release of Information" statement on the CMS-1500 claim.
7. Identify two classifications of patients who are not required to sign the "Authorization for Release of Information" statement on the CMS-1500 claim.
8. Explain how the patient authorization for release of information is obtained for electronic claims.
9. Verify a legitimate telephone request for patient information.
10. Process facsimile (fax) requests for patient information.
11. Prepare a confidentiality notice to serve as the first page of faxed patient information.
12. Establish a patient record retention policy for the physician's office.
13. Summarize the *CMS Internet Security Policy* and the *Stark II regulations*.
14. List the components of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and explain the health care impact of each.
15. Outline the elements of the *Compliance Program Guidance for Physician Practices* and the *Payment Error Prevention Program*.
16. Implement *CMS's National Correct Coding Initiative* (CCI).
17. Provide an example of *unbundling*.
18. Differentiate among the NPI, PlanID, EIN, and patient identifier.
19. List the scheduled implementation dates for CMS's *electronic health care standards* and *privacy standards*.
20. Explain how overpayments are recovered.

INTRODUCTION

The health insurance specialist must be knowledgeable about laws and regulations for maintaining patient records and processing health insurance claims. This chapter defines legal and regulatory terminology and summarizes laws and regulations that affect health insurance processing. Internet links are also included as a resource for remaining up-to-date and obtaining clarification of legal and regulatory considerations.

INTRODUCTION TO LEGAL AND REGULATORY CONSIDERATIONS

Federal and state **statutes** (or **statutory law**) are laws passed by legislative bodies (e.g., federal congress and state legislatures). These laws are then implemented as **regulations**, which are guidelines written by administrative agencies (e.g., CMS). **Case law** (or **common law**) is based on court decisions that establish a **precedent** (or standard).

Federal regulations govern programs such as Medicare, Medicaid, TRICARE, and the Federal Employees Health Benefit Plans (FEHBP). State laws regulate insurance companies, patient record keeping practices, and provider licensing. State insurance departments determine coverage issues for insurance policies (contracts) and state workers' compensation plans.

Civil law deals with all areas of the law that are not classified as criminal. **Criminal law** is public law governed by statute or ordinance that deals with crimes and their prosecution. A **subpoena** is an order of the court that requires a witness to appear at a particular time and place to testify. A **subpoena duces tecum** requires documents (e.g., patient record) be produced. A subpoena is used to obtain witness testimony at trial and at **deposition**, which is testimony under oath taken outside of court (e.g., at the provider's office). In civil cases (e.g., malpractice), the provider might be required to complete an **interrogatory**, which is a document containing a list of questions that must be answered in writing.

Qui tam is an abbreviation for the Latin phrase *qui tam pro domino rege quam pro sic ipso in hoc parte sequitur* meaning "who as well for the king as for himself sues in this matter." It is a provision of the Federal Civil False Claims Act, which allows a private citizen to file a lawsuit in the name of the U.S. Government charging fraud by government contractors and other entities that receive or use government funds, and share in any money recovered. A common defendant in *qui tam* actions involving Medicare/Medicaid fraud includes physicians, hospitals, HMOs, and clinics.

To accurately process health insurance claims, especially for government programs like Medicare and Medicaid, you should become familiar with the *Code of Federal Regulations* (Figure 5-1). Providers and health insurance specialists can locate legal and regulatory issues found in such publications as the *Federal Register* and *Medicare Bulletin*. The ***Federal Register*** (Figure 5-2) is a legal newspaper published every business day by the National Archives and Records Administration (NARA). It is available in paper form, on microfiche, and online.

Title 42--Public Health

CHAPTER IV--CENTERS FOR MEDICARE & MEDICAID SERVICES, DEPARTMENT OF HEALTH AND HUMAN SERVICES

PART 405--FEDERAL HEALTH INSURANCE FOR THE AGED AND DISABLED

FIGURE 5-1 Portion of table of contents from Code of Federal Regulations, Title 42, Public Health, Chapter IV, Centers for Medicare & Medicaid Services (Reprinted according to National Archives and Records Administration Permissions Notice)

The ***Medicare Bulletin*** (Figure 5-3) is published by CMS as a legal notice to providers (e.g., physicians, suppliers, and so on) about requirements imposed by Medicare laws, regulations, and guidelines. It is mailed to providers by their Medicare **carrier**, which is the organization (e.g., insurance company) that contracts with CMS to process Medicare Part B claims. (Hospitals receive the *Medicare Bulletin* from their **fiscal intermediary (FI)**, which is the organization that contracts with CMS to process Medicare Part A claims.)

NOTE: Health care organizations should appoint one individual to review CMS transmittals (e.g., *Medicare Bulletin*), update the Medicare carriers manual, and educate staff about changes.

EXAMPLE 1: FEDERAL STATUTE, IMPLEMENTED AS STATE PROGRAM

Congress passed Title XXI of the Social Security Act as part of the Balanced Budget Act of 1997, which called for implementation of the State Children's Health Insurance Program. In response, New York implemented Child Health Plus, which expanded insurance eligibility to children under age 19 who are not eligible for Medicaid and have limited or no health insurance. Even if family income is high, children can be eligible to enroll in Child Health Plus; an insurance premium in the form of a monthly family contribution may be required (e.g., a family of two with an income ranging from $24,977–$25,920 pays $15.00 per month per child).

Exposure Cohort Petitioning Process

Procedures, NIOSH-IREP concerns and model transparency, dose reconstruction workgroup discussion and issues, and Board discussion.

Agenda items are subject to change as priorities dictate.

For Further Information Contact: Larry Elliott, Executive Secretary, ABRWH, NIOSH, CDC, 4676 Columbia Parkway, Cincinnati, Ohio 45226, telephone (513) 841–4498, fax (513) 458–7125.

The Director, Management Analysis and Services Office, has been delegated the authority to sign **Federal Register** notices pertaining to announcements of meetings and other committee management activities for both the Centers for Disease Control and Prevention and the Agency for Toxic Substances and Disease Registry.

Dated: June 12, 2002.

John C. Burckhardt,

Acting Director, Management Analysis and Services Office, Centers for Disease Control and Prevention.

[FR Doc. 02–15273 Filed 6–14–02; 8:45 am]

BILLING CODE 4163–19–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services
Privacy Act of 1974; Report of Modified or Altered System

AGENCY: Centers for Medicare & Medicaid Services (CMS), (formerly the Health Care Financing Administration), Department of Health and Human Services (HHS).

ACTION: Notice of proposal to modify or alter a System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter an SOR, ''End Stage Renal Disease (ESRD) Program Management and Medical Information System (PMMIS),'' System

No. 09–70–0520. We propose to broaden the scope of this system to include the collection and maintenance of ESRD Core Indicators or Clinical Performance Measures (CPM). Data contained in CPM Data Set are being added to meet statutory requirements and to augment the usefulness of the information for research, quality improvement projects, and policy formulation. We are deleting routine use number 2 authorizing disclosures to organizations deemed qualified to carry out quality assessments; number 5, authorizing disclosures to a contractor; number 6, authorizing disclosures to an agency of a state government; and an unnumbered routine use which authorizes the release of information to the Social Security Administration (SSA).

Routine use number 2 is being deleted because it is not clear what ''organizations'' are being identified and who should receive information referred to in this routine use. We will add a new routine use to accomplish release of information in this system to ESRD Network Organizations and Quality Improvement Organizations (QIO) to carry out quality assessments, medical audits, quality improvement projects, and/or utilization reviews. Disclosures allowed by routine use number 6 and to SSA will be covered by a new routine use to permit release of information to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Disclosures previously allowed by routine use number 5 will now be covered by proposed routine use number 1.

The security classification previously reported as ''None'' will be modified to reflect that the data in this system is considered to be ''Level Three Privacy Act Sensitive.'' We are modifying the language in the remaining routine uses to provide clarity to CMS' intention to disclose individual-specific information contained in this system. The proposed routine uses will be prioritized and reordered according to their proposed usage. We will also update any sections of the system that were affected by the recent reorganization and update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of the system of records is to maintain information on Medicare ESRD beneficiaries, non-Medicare ESRD patients, Medicare approved ESRD hospitals and dialysis facilities, and Department of Veterans Affairs (DVA) patients. The ESRD/ PMMIS is used by CMS and the renal community to perform their duties and responsibilities in monitoring the Medicare status, transplant activities, dialysis activities, and Medicare utilization (inpatient and physician/supplier bills) of ESRD patients and their Medicare providers, as well as in calculating the Medicare covered periods of ESRD. Information retrieved from this system of records will also be disclosed to:

FIGURE 5-2 Sample page from the *Federal Register* (Reprinted according to National Archives and Records Administration Permissions Notice)

PROGRAM MEMORANDUM

Department of Health and Human Services
Centers for Medicare & Medicaid Services

INSURANCE COMMISSIONERS
INSURANCE ISSUERS

Transmittal No. 02-01 **Date** March 2002

Title: Medigap Insurance Standards Bulletin Series — INFORMATION

Subject: Processing Applications for Medigap Guaranteed Issue Policies and Policies Sold during Open Enrollment Periods

Market: Medigap

I. PURPOSE

The purpose of this bulletin is to clarify the interpretation of certain statutory requirements of sections 1882(s)(2) and (3) of the Social Security Act (the Act). These sections govern a Medicare beneficiary's right to purchase a Medicare supplemental policy (commonly referred to as a Medigap policy) during the six-month Medigap open enrollment period, or on a guaranteed issue basis when certain circumstances apply.

Specifically, this bulletin will focus on the actions an issuer is required to take when an applicant has federally-mandated open enrollment or guaranteed issue rights. This bulletin does not address issues that have arisen about how to determine **whether** an individual has open enrollment or guaranteed issue rights. Rather, it specifies the issuer's obligations with respect to beneficiaries who clearly have those rights.

II. BACKGROUND

Section 1882(s)(2) of the Act requires an issuer to make available any Medigap policy it sells in a state to any Medicare beneficiary during the first six months the individual is both age 65 or older and is enrolled in Part B of Medicare. During the Medigap open enrollment period, an issuer may not deny or condition the issuance or effectiveness of a Medigap policy, or discriminate in the pricing of the policy because of health status, claims experience, receipt of health care, or medical condition.

FIGURE 5-3 Sample *Medicare Bulletin* (Reprinted in accordance with CMS Content Reuse policy)

EXAMPLE 2: FEDERAL STATUTE, IMPLEMENTED AS A FEDERAL REGULATION, AND PUBLISHED IN THE *FEDERAL REGISTER*

Congress passed the Balanced Budget Refinement Act of 1999 (Public Law 106-113), which called for a number of revisions to Medicare, Medicaid, and the State Children's Health Insurance Program. On May 5, 2000, the Department of Health and Human Services published a proposed rule in the *Federal Register* to revise the Medicare hospital inpatient prospective payment system for operating costs. This proposed rule was entitled "Medicare Program; Changes to the Hospital Inpatient Prospective Payment Systems and Fiscal Year 2001 Rates; Proposed Rule." The purpose of publishing the proposed rule is to allow for comments from health care providers. Once the comment period has ended, the final rule is published in the *Federal Register*.

EXAMPLE 3: CASE LAW

When originally passed, New York State Public Health Law (PHL) sections 17 and 18 allowed a *reasonable charge* to be imposed for copies of patient records.

Health care facilities, therefore, charged fees for locating the patient's record and making copies. These fees were later challenged in court, and reasonable charge language in the PHL was interpreted in *Hernandez v. Lutheran Medical Center* (1984), *Ventura v. Long Island Jewish Hillside Medical Center* (1985), and *Cohen v. South Nassau Communities Hospital* (1987). The interpretation permitted charges of $1.00 to $1.50 per page, plus a search and retrieval fee of $15.

NOTE: Sections 17 and 18 of the PHL were amended in 1991 when the phrase, "the reasonable fee for paper copies shall not exceed seventy-five cents per page" was added to the law.

INTERNET LINKS

The *Federal Register* can be accessed online at http://www.archives.gov

CMS press releases can be viewed at http://www.cms.gov

Medicare bulletins can be viewed at a carrier's or fiscal intermediary's official Web site. The Trailblazer Health Enterprises, LLC™ Medicare site can be viewed at http://www.trailblazerhealth.com

Consider subscribing to an online service, such as CodeCorrect.com located at http://www.codecorrect.com, that posts up-to-date billing and coding news. Most online services provide a free trial membership to try out their products before actually purchasing them.

State departments of health Web sites can be accessed at http://www.cdc.gov by clicking on the Other Sites link.

Membership in professional associations can also prove helpful in accessing up-to-date information about the health insurance industry (refer to Chapter 1 for information on joining professional associations). Newsletters and journals published by professional associations routinely include articles that clarify implementation of new legal and regulatory issues. They also provide resources for obtaining the most up-to-date information about such issues. Another way to remain current is to subscribe to a **listserv**, which is a subscriber-based question-and-answer forum that is available through e-mail.

INTERNET LINKS

CMS offers free subscriptions to electronic mailing listservs at http://cms.hhs.gov/medlearn/listserv.asp. Notices are sent to your e-mail address.

Join Medicare Part-B listserv at http://lyris.ucg.com/cgi-bin/listserv/listserv.pl/ partb-l. This listserv is very active (50+ postings per day), and you may want to join the digest version to receive one daily e-mail that contains all postings for that day.

CONFIDENTIALITY OF PATIENT INFORMATION

Confidentiality of patient information includes the related concepts of privacy and security. **Privacy** is the right of individuals to keep their information from being dis-

closed to others. Once information is disclosed (e.g., for the purpose of obtaining health care), it is essential that confidentiality of the information be maintained. **Confidentiality** involves restricting patient information access to those with proper authorization and maintaining the security of patient information. **Security** involves the safekeeping of patient information by:

- controlling access to hard copy and computerized records (e.g., implementing password protection for computer-based patient records).
- protecting patient information from alteration, destruction, tampering, or loss (e.g., establishing office policies).
- providing employee training in confidentiality of patient information (e.g., conducting annual in-service education programs).
- requiring employees to sign a confidentiality statement that details the consequences of not maintaining patient confidentiality (e.g., employee termination).

Because patient information is readily available through computerized databases and other means, it is essential to take steps to maintain confidentiality. **Breach of confidentiality**, often unintentional, involves the unauthorized release of patient information to a third party. Examples include:

- discussing patient information in public places (e.g., elevators).
- leaving patient information unattended (e.g., computer screen display).
- communicating patient information to family members without the patient's consent.
- publicly announcing patient information in a waiting room or registration area.
- accessing patient information without a job-related reason.

To understand the legality of this issue, it is first necessary to define contract and third party. A **contract** is an agreement between two or more parties to perform specific services or duties. A **third party** is one who is not involved in the patient/provider relationship. (The **first party** is the person designated in the contract to receive a contracted service. The **second party** is the person or organization providing the service.)

A **verbal contract** is established between the patient and the health care provider when the patient asks a provider to perform medical services. In exchange for services, the patient agrees to promptly pay the provider's customary fee for those services. The parties to this contract are the patient, the health care provider, and the office staff. If the patient is a minor or a legally incompetent adult, parents or stated **guardian(s)** (the person(s) legally designated to be in charge of the patient's affairs) contract for the services of the health care provider on behalf of the patient. The parents or guardians, therefore, become a party to the *patient-health care provider contract*.

For patients to receive proper treatment they must be willing to be examined and touched by medical professionals. Patients must also reveal the reason they sought medical advice and how this problem has affected them. At times, this requires the patient to reveal intimate thoughts and feelings, as well as their bodies. If the patient is to feel comfortable in confiding to a health care provider, the patient must be assured that the office will protect and control the confidential information given to the health care provider. Breach of confidentiality cannot be charged against a health care provider if written permission to release necessary medical

information to an insurance company or other third party has been obtained from the patient, the parent, or the guardian. A good maxim to follow is:

"When in doubt, have them write it out."

Authorized Release of Information to Payers

To prevent breach of patient confidentiality, all health care professionals involved with processing insurance claims of the CMS-1500 should check to be sure the patient has signed an "Authorization for Release of Medical Information" statement before completing the claim. The release can be obtained in one of two ways:

- Ask the patient to sign block 12, Patient's or Authorized Person's Signature, on the CMS-1500 claim (Figure 5-4) or
- Ask the patient to sign a special release form that is customized by each practice and specifically names the patient's insurance company (Figure 5-5).

NOTE: Computerized practices must obtain the patient's signature on the special release form and provide a copy to the patient's insurance company upon request. With this method, the CMS-1500 claim generated will contain SIGNATURE ON FILE in Block 12 (Figure 5-6).

NOTE: A dated, signed special release form is generally considered valid for one year. Be sure to obtain the patient's signature on the special release form each year. Undated signed forms are assumed to be valid until revoked by the patient or guardian. CMS regulations permit government programs to accept both dated and undated authorizations.

Established medical practices must update patient information and obtain the necessary authorization forms. Patients who regularly seek care must sign a new authorization each year.

Authorization Exceptions

The federal government allows three exceptions to the required authorization for release of medical information to insurance companies:

1. Patients covered by Medicaid
2. Patients covered by Workers' Compensation
3. Patients seen by a provider in a hospital, but who do not receive follow-up care in the provider's office

READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.
12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE I authorize the release of any medical or other information necessary to process this claim. I also request payment of government benefits either to myself or to the party who accepts assignment below.

SIGNED Mary Sue Patient DATE

FIGURE 5-4 Patient signature in Block 12

(Insert Letterhead)

Authorization for Release of Medical Information to the Payer and Assignment of Benefits to Physician

COMMERCIAL INSURANCE

I hereby authorize releaase of medical information necessary to file a claim with my insurance company and ASSIGN BENEFITS OTHERWISE PAYABLE TO ME TO _____*(fill in provider's name)*_____

I understand that I am financially responsible for any balance not covered by my insurance carrier. A copy of this signature is as valid as the original.

Signature of patient or guardian_____ Date _____

MEDICARE

BENEFICIARY _____ Medicare Number _____

I request that payment of authorized medicare benefits be made on my behalf to _____*(fill in provider's name)*_____ for any service furnished to me by that provider. I authorize any custodian of medical information about me to release to the Centers for Medicare & Medicaid Services and its agents any information needed to determine these benefits or the benefits payable for related services.

Beneficiary Signature _____ Date _____

MEDICARE SUPPLEMENTAL INSURANCE

BENEFICIARY _____ Medicare Number _____

Medigap ID Number _____

I hereby give _____*(Name of Physician or Practice)*_____ permission to bill for Medicare Supplemental Insurance payments for my medical care.

I understand that _____*(Name of Medicare Supplemental Insurance Carrier)*_____ needs information about me and my medical condition to make a decision about these payments. I give permission for that information to go to _____*(Name of Medicare Supplemental Insurance Company)*_____ .

I request that payment of authorized Medicare Supplemental benefits be made either to me or on my behalf to (Name of Physician or Practice) for any services furnished me by that physician. I authorize any holder of medical information about me to release to (Name of Medicare Supplemental Insurance Company) any information required to determine and pay these benefits.

Beneficiary Signature _____ Date _____

FIGURE 5-5 Sample authorization form for release of medical information and assignment of benefits

READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.

12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE I authorize the release of any medical or other information necessary to process this claim. I also request payment of government benefits either to myself or to the party who accepts assignment below.

SIGNED SIGNATURE ON FILE DATE _____

13. INSURED'S OR AUTHORIZED PERSON'S SIGNATURE I authorize payment of medical benefits to the undersigned physician or supplier for services described below.

SIGNED _____

FIGURE 5-6 Release of medical information (Blocks 12 and 13 on a CMS-1500 claim)

For the first two exceptions, the federal government mandated that when a patient enrolls in Medicaid or requests benefits under the Workers' Compensation program, the patient becomes a third-party beneficiary in a contract between the health care provider and the government agency that sponsors the specific program. When health care providers agree to treat either a Medicaid or a Workers' Compensation case, they agree to accept the program's payment as payment in full for covered procedures rendered to these patients. The patient may be billed only if services rendered are not covered by the payer, or if the payer determines the patient was ineligible for benefits on the date(s) of service.

For the third exception, patients are required to sign an authorization for treatment and an authorization for release of medical information at the hospital before being treated by the hospital or seen by the provider. If the hospital's medical information release form includes both the authorization for release of information from the hospital and the treating physician's services, claims may be submitted by the physician's office without obtaining a separate medical information release from the patient. The words SIGNATURE ON FILE are entered in Block 12 of the CMS-1500 claim filed by the provider (Figure 5-6). If, at a later date, proof of the signature authorizing the release of information is requested, a copy of the signed authorization may be obtained from the hospital's files.

Release of HIV/AIDS Status

Patients who undergo screening for the human immunodeficiency virus (HIV) or AIDS infection should sign an additional authorization statement for release of information regarding their HIV/AIDS status (Figure 5-7). Several states require very specific wording on this form. Be sure to determine if your state requires a special form.

(Insert letterhead)

Authorization to Release HIV-Related Information

Patient Name _____ Date of Service _____

Address _____ Date of Birth _____

I authorize _____*(name of practice)*_____ to release HIV-related information to the following organization for the purpose of processing payment for services rendered. I understand that this is a required consent and I voluntarily and knowingly sign this authorization for release of information to:

Name of Requestor _____

Address _____

I understand this consent can be cancelled at any time, but that information already disclosed is exempt. I release _____*(name of practice)*_____ from any liability arising from the release of information to the individual or agency stated above.

Patient signature: _____ Date: _____

Patient representative signature: _____ Date: _____

Reason patient is unable to sign: _____

Witness signature: _____ Date: _____

Information released shall include a statement prohibiting the requestor from redisclosing patient information without the prior consent of the patient. Unless otherwise specified, *this authorization will expire one year from date signed.*

FIGURE 5-7 Sample authorization to release HIV-related information

Release of Information to Other Third Parties

The patient's signature on the release of medical information form restricts the release of information to the party specified. Release of the same information or copies of the patient medical record to any other third party is not authorized. To release medical information to an individual other than the payer, be sure to have the patient complete an authorization to release medical information (Figure 5-8).

Most states have special laws covering release of mental health services records. There also are federal laws covering confidentiality when the patient is enrolled in a federally assisted alcohol and drug abuse program. If you work with a substance abuse facility or have a patient receiving mental health services, acquaint yourself with federal and state laws.

Need To Know Rule

Confidentiality is breached when a health care professional in the practice releases confidential information to a person who has no demonstrable legal need to receive this information. Persons in this category may include spouses, friends, relatives, other patients, or colleagues working in a practice where the patient has had no previous contact.

NOTE: There is a demonstrable need to provide limited patient information to office personnel when making a referral of a patient to that office.

(Insert letterhead)

Authorization to Release Medical Information

Patient Name _____ Date of Service _____

Address _____ Date of Birth _____

I authorize _____*(name of practice)*_____ to release information contained in my medical record concerning treatment provided from _____ to _____ . I understand that this is a required consent and I voluntarily and knowingly sign this authorization for release of information to:

Name of Requestor _____

Address _____

I release _____*(name of practice)*_____ from any liability arising from the release of information to the individual or agency stated above.

Patient signature: _____ Date: _____

Patient representative signature: _____ Date: _____

Reason patient is unable to sign: _____

Witness signature: _____ Date: _____

Information released shall include a statement prohibiting the requestor from redisclosing patient information without the prior consent of the patient.

FIGURE 5-8 Sample authorization to release general medical information

This does not preclude the sharing of case studies or specific insurance billing problems with colleagues or acquaintances. In these discussions, however, great care must be taken to ensure that a third party (a person or entity not involved in the patient-provider relationship) cannot identify the patient or family involved.

EXAMPLE: Mary Sue Patient is seen in Dr. Day's office with the complaint of abdominal pain. After examining the patient and evaluating test results, Dr. Day refers Mary Sue to Dr. Shaw, a gastroenterologist. Dr. Day's medical assistant schedules the patient's appointment with Dr. Shaw. According to individual state law, only **minimum data** may be shared with Dr. Shaw's office, which means enough information to schedule the appointment (e.g., reason for the referral and office visit).

NOTE: Each state defines what is meant by *minimum data*. The HIPAA Privacy Rule also specifies that the minimum amount of information necessary for the purpose of the use or disclosure is to be disclosed.

CLAIMS INFORMATION TELEPHONE INQUIRIES

Another area of concern regarding breach of confidentiality involves the clarification of insurance data by telephone. A signed release statement from the patient may be on file, but the office has no assurance of the identity or credentials of the inquirer. It is very simple for a curious individual to place a call to a physician's office and claim to be an insurance company benefits clerk. The rule to follow here is:

Never give information over the phone or in person until you have verified that the party making the request is entitled to the information.

To verify insurance company telephone inquiries for clarification of claims data, place the caller on hold until you have the file copy of the patient's insurance claim in hand. Ask the caller to read the line on the claim that needs clarification. When sufficient information from the caller's copy is obtained to ensure validity of the inquiry, clarifying statements or data may be released by phone. Be sure to follow up this action by writing a memo detailing the conversation, and file it with the practice's file copy of the claim. Computerized practices should access the patient account and/or demographic screens to confirm the data. If an error is detected, it should be corrected and a notation made to explain the change in the message section of the patient's computer file.

If there are multiple questions or if a detailed clarification is needed, it is best to ask for a written request for information. The written request and a copy of the response then become an official addendum to the practice's file copy of the claim.

Another way to verify a caller's identity is to use a "Caller ID" service. You should also ask how you can return the call. Then, place the call through the caller's switchboard to verify that the caller was a valid insurance company employee. If verification cannot be made, the caller must submit a request in writing on company stationery.

Phone Requests from Lawyers

Great care should be taken when attorneys request information over the telephone. Lawyers are well aware that offices must have the patient's signed release of information in the practice's files before answering questions. Never assume that the

attorney has a signed release from the patient, and do not submit to pressure from the attorney to breach confidentiality.

Law offices are required to send any patient's authorized release of information statement the lawyers have obtained to the provider. After comparing and matching the signature on the release form sent by the lawyer with the patient's or guardian's signature and handwriting on the registration form, you should respond to the lawyer's request in writing.

FACSIMILE TRANSMISSION

Great care must be taken to ensure that sensitive information sent by fax reaches the intended receiver and is handled properly. It is recommended that health information be faxed only when there is:

1. an urgent need for the health record and mailing the record will cause unnecessary delays in treatment, or
2. immediate authorization for treatment is required from a primary care physician or other third-party case manager.

In such cases, information transmitted should be limited only to the information required to satisfy the immediate needs of the requesting party. Each transmission of sensitive material should have a cover sheet including the following information:

- Name of the facility to receive the facsimile
- Name and phone number of the person authorized to receive the transmission
- Name and phone number of the sender
- Number of pages being transmitted
- A confidentiality notice or disclaimer (Figure 5-9)
- Instructions to authorized recipient to send verification of receipt of transmittal to the sender.

The practice should keep a dated log of the transmission of all medically sensitive facsimiles and copies of all "receipt of transmittal" verifications signed and returned by the authorized recipient. Special care must be taken to ensure that proper facsimile destination numbers are keyed into the fax machine prior to transmission.

If you have received this transmittal in error, please notify the sender immediately.

The material in this transmission contains confidential information that is legally privileged. This information is intended only for the use of the individual or entity named above.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken based on the contents of this transmission is strictly prohibited.

FIGURE 5-9 Sample fax confidentiality notice

CONFIDENTIALITY AND THE INTERNET

At present there is no guarantee of confidentiality when patient records are transmitted via the Internet. If time constraints prevent sending sensitive information through a more secure delivery system, special arrangements may be made with the requesting party to transmit the document after deleting specific patient identification information. It is best to call the party requesting the documents to arrange for an identifier code to be added to the document so that the receiving party is assured that the information received is that which was requested. This transmission should be followed by an official unedited copy of the record sent by overnight delivery including specific patient material that was deleted in the previous transmission.

On November 24, 1998, the *HCFA Internet Security Policy* issued guidelines for the security and appropriate use of the Internet for accessing and transmitting sensitive information (e.g., Medicare beneficiary information). The information must be **encrypted** so that information is converted to a secure language format for transmission, and authentication or identification procedures must be implemented to assure that the sender and receiver of data are known to each other and are authorized to send and/or receive such information.

RETENTION OF PATIENT INFORMATION AND HEALTH INSURANCE RECORDS

OBRA of 1987 requires patient information and health insurance records to be maintained for six years, unless state law specifies a longer period. The records must be available as references for use by CMS, fiscal intermediaries, DHHS audit, or as designated for billing review and other references. It is acceptable to microfilm patient information and insurance records (including attachments submitted to insurance companies), if the microfilm accurately reproduces all original documents. All other categories of health insurance records are to be maintained in their original form.

EMPLOYEE RETIREMENT INCOME SECURITY ACT (ERISA)

The *Employee Retirement Income Security Act (ERISA)* was enacted in 1974 to ensure that pension and other benefits were provided to employees as promised by their employers. ERISA rules cover pensions, profit-sharing stock bonuses, health care, life insurance, prepaid legal services, and disability insurance (both long- and short-term). The Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA) amended ERISA to include provisions for continuation of health care, which apply to group health plans of employers with 20 or more employees. Participants and beneficiaries have the right to maintain, at their own expense, health care plan coverage that would be lost due to a triggering event (e.g., termination of employment). The cost of this coverage is to be comparable to what it would be if they were still members of the employer's group. Individuals are required to receive an initial general notice informing them of their rights under COBRA. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) further amended ERISA to improve the portability and continuity of health insurance coverage in connection with employment. Provisions include rules relating to pre-existing conditions, exclusions, special enrollment rights, and prohibition of discrimination against individuals based on health status-related factors.

MEDICAL NECESSITY

Today's concept of medical necessity determines the extent to which individuals with health conditions receive health care services. (The concept was introduced in the 1970s when health insurance contracts intended to exclude care, such as voluntary hospitalizations prescribed primarily for the convenience of the provider or patient.) *Medical necessity* is the measure of whether a health care procedure or service will be reimbursed by a payer, and this decision-making process is based on the payer's contractual language and the treating provider's documentation. Generally the following criteria are used to determine medical necessity:

- *Purpose:* the procedure or service is performed to treat a medical condition
- *Scope:* the most appropriate level of service is provided, taking into consideration potential benefit and harm to the patient
- *Evidence:* the treatment is known to be effective in improving health outcomes
- *Value:* the treatment is cost-effective for this condition when compared to alternative treatments, including no treatment.

NOTE: Cost-effective does not necessarily mean least expensive.

FEDERAL FALSE CLAIMS ACT

The federal government passed the **Federal False Claims Act** during the Civil War to regulate fraud associated with military contractors selling supplies and equipment to the Union Army. Since then, this Act has been used by federal agencies to regulate the conduct of any contractor submitting claims for payment to the federal government for any program, including Medicare. Control of fraud and abuse has been a key regulatory interest ever since the hospital prospective payment system legislation (called Diagnosis Related Groups, or DRGs) was passed as part of the Tax Equity & Fiscal Responsibility Act (TEFRA) of 1982. Prior to TEFRA, the cost-based reimbursement system for Medicare claims made fraud almost unnecessary because the system rewarded high utilization of services. The implementation of DRGs resulted in the first serious "gaming" of the system to find ways to maximize revenues for hospitals. Because the diagnosis and procedure codes reported impact the DRG selected (and resultant payment), some hospitals engaged in a practice called **upcoding**, which is the assignment of an ICD-9-CM diagnosis code that does not match patient record documentation for the purpose of illegally increasing reimbursement (e.g., assigning the ICD-9-CM code for heart attack code when angina was actually documented in the record). As a result, upcoding became a serious fraud concern under DRGs.

Stark II Regulations

In the 1980's, the issue of self-referral was presented as a serious legislative item in Congress. **Self-referral** involves providers ordering services to be performed for patients by organizations in which they have a financial interest (e.g., laboratories, or durable medical equipment). Commercial laboratories were targeted first, followed by most methods of physician or provider investment in health care delivery entities. Representative Stark led legislative efforts to treat any types of referral practices by physicians to entities in which they had a material financial interest as fraud. Examples of material financial interest include ownership interest and kickbacks to induce referrals (e.g., free or less than fair market value terms for office space, consulting services, and practice management). In 1998, **Stark II regulations** were

released for implementation to regulate physician referral for Medicare services from which the doctor profits. Studies revealed that when a doctor has an investment interest in a lab, for example, the doctor orders more tests and more expensive services.

Hospitals are also required to comply with the Stark II self-referral law because of relationships they establish with physicians. They must make sure that the financial arrangements they make with physicians who refer patients to them (e.g., inpatient admissions, and outpatient services) conform to exceptions to the Stark II law (e.g., personal service exception, space lease exception, and equipment lease exception). In addition, hospitals should make sure that contracts are negotiated for hospital-physician relationships.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) due to additional concerns about fraud (e.g., coding irregularities, medical necessity issues, and waiving of copays and deductibles). While the Federal False Claims Act provided HCFA with regulatory authority to enforce fraud and abuse statutes for the Medicare program, HIPAA extends that authority to all federal and state health care programs.

The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, Public Law 104-191, amended the Internal Revenue Code of 1986, to:

- improve the portability and continuity of health insurance coverage in the group and individual markets.
- combat waste, fraud, and abuse in health insurance and health care delivery.
- promote the use of medical savings accounts.
- improve access to long-term care services and coverage.
- simplify the administration of health insurance by creating unique identifiers for providers, health plans, employers, and individuals.
- create standards for electronic health information transactions.
- create privacy standards for health information.

A discussion on each HIPAA component follows, and although HIPAA standards are still being finalized, health care organizations should develop and implement a response to each component.

INTERNET LINKS

CMS business activities with regard to HIPAA can be found at http://.cms.gov/hipaa

Educate your staff about HIPAA and Medicare issues. Download free interactive computer-based training courses and learn about satellite programs designed to teach Medicare billing guidelines at http://.cms.hhs.gov/medlearn.

Portability and Continuity of Health Insurance Coverage

HIPAA provisions were designed to improve the portability and continuity of health coverage by:

- limiting exclusions for pre-existing medical conditions.
- providing credit for prior health coverage and a process for transmitting certificates and other information concerning prior coverage to a new group health plan or issuer.
- providing new rights that allow individuals to enroll for health coverage when they lose other health coverage, change from group to individual coverage, or have a new dependent.
- prohibiting discrimination in enrollment and premiums against employees and their dependents based on health status.
- guaranteeing availability of health insurance coverage for small employers and renewability of health insurance coverage in both the small and large group markets.
- preserving, through narrow preemption provisions, the states' traditional role in regulating health insurance, including state flexibility to provide greater protections.

Fraud and Abuse

HIPAA defines **fraud** as "an intentional deception or misrepresentation that someone makes, knowing it is false, that could result in an unauthorized payment." The attempt itself is considered fraud, regardless of whether it is successful. **Abuse** "involves actions that are inconsistent with accepted, sound medical, business, or fiscal practices. Abuse directly or indirectly results in unnecessary costs to the program through improper payments." The difference between fraud and abuse is the individual's intent; however, both have the same impact in that they steal valuable resources from the health care industry. The most common forms of Medicare fraud include:

- billing for services not furnished.
- misrepresenting the diagnosis to justify payment.
- soliciting, offering, or receiving a kickback.
- unbundling codes (reporting multiple CPT codes to increase reimbursement, when a single combination code should be reported).
- falsifying certificates of medical necessity, plans of treatment, and medical records to justify payment.
- billing for a service that was not furnished.

Examples of abuse include:

- excessive charges for services, equipment, or supplies.
- submitting claims for items or services that are not medically necessary to treat the patient's stated condition.
- improper billing practices that result in a payment by a government program when the claim is the legal responsibility of another third-party payer.
- violations of participating provider agreements with insurance companies.

When a Medicare provider commits fraud, an investigation is conducted by the Department of Health and Human Services (DHHS) Office of the Inspector General (OIG). The OIG Office of Investigations prepares the case for referral to the Department of Justice for criminal and/or civil prosecution. A person found guilty of Medicare fraud faces criminal, civil, and/or administrative sanction penalties including:

- civil penalties of $5,000 to $10,000 per false claim plus triple damages under the False Claims Act. (The provider pays an amount equal to three times the claim submitted in addition to the civil penalties fine.)
- criminal fines and/or imprisonment of up to ten years if convicted of the crime of health care fraud as outlined in HIPAA or, for violations of the Medicare/Medicaid Anti-Kickback Statute, imprisonment of up to five years and/or a criminal fine of up to $25,000.
- administrative sanctions including up to a $10,000 civil monetary penalty per line item on a false claim, assessments of up to triple the amount falsely claimed, and/or exclusion from participation in Medicare and state health care programs.

In addition to the penalties outlined above, those who commit health care fraud can also be tried for Mail and Wire Fraud.

EXAMPLE: Medical review of claims submitted to Medicare by a physician group practice that contains mental health providers identified a pattern of psychiatric services billed on behalf of nursing facility patients with a medical history of dementia. Review of patient record documentation revealed no mental health care physician orders or plans of treatment. This is an example of billing for services not furnished.

The DHHS Office of Inspector General (OIG) published the final *Compliance Program Guidance for Individual and Small Group Physician Practices* in the October 5, 2000 *Federal Register*. The intent of the guidance is to help physicians in individual and small group practices design voluntary compliance programs that best fit the needs of individual practices. By law, physicians are not subject to civil, administrative or criminal penalties for innocent errors, or even negligence. The civil False Claims Act covers only offenses that are committed with *actual knowledge* of the falsity of the claim, *reckless disregard* or *deliberate ignorance* of the truth or falsity of a claim. (The False Claims Act does not cover mistakes, errors or negligence.) The OIG has stated that it is mindful of the difference between innocent errors (e.g., erroneous claims) and reckless or intentional conduct (e.g., fraudulent claims).

A voluntary compliance program can help physicians identify erroneous and fraudulent claims by ensuring that submitted claims are true and accurate, expediting and optimizing proper payment of claims, minimizing billing mistakes, and avoiding conflicts with self-referral and antikickback statutes. Unlike other guidance previously issued by the OIG (e.g., *Third-Party Medical Billing Company Compliance Program Guidance*), the final physician guidance does not require that physician practices implement all seven standard components of a full scale compliance program. (While the seven components provide a solid basis upon which a physician practice can create a compliance program, the OIG acknowledges that full implementation of all components may not be feasible for smaller physician practices.) Instead, the guidance emphasizes a step-by-step approach for those practices to follow in developing and implementing a voluntary compliance program.

As a first step, physician practices can begin by identifying risk areas which, based on a practice's specific history with billing problems and other compliance

issues, might benefit from closer scrutiny and corrective/educational measures. The step-by-step approach is as follows:

1. Perform periodic audits to internally monitor billing practices.
2. Develop written practice standards and procedures.
3. Designate a compliance officer to monitor compliance efforts and enforce practice standards.
4. Conduct appropriate training and education about practice standards and procedures.
5. Respond appropriately to detected violations by investigating allegations and disclosing incidents to appropriate government entities.
6. Develop open lines of communication (e.g., discussions at staff meetings regarding erroneous or fraudulent conduct issues) to keep practice employees updated regarding compliance activities.
7. Enforce disciplinary standards through well-publicized guidelines.

The final guidance further identifies four specific compliance risk areas for physicians: (1) proper coding and billing; (2) ensuring that services are reasonable and necessary; (3) proper documentation; and (4) avoiding improper inducements, kickbacks and self-referrals. These risk areas reflect areas in which the OIG has focused its investigations and audits related to physician practices. The final guidance also provides direction to larger practices in developing compliance programs by recommending that they use both the physician guidance and previously issued guidance, such as the *Third-Party Medical Billing Company Compliance Program Guidance* or the *Clinical Laboratory Compliance Program Guidance*, to create a compliance program that meets the needs of the larger practice.

INTERNET LINK

The OIG Fraud Prevention and Detection program is available at http://oig.hhs.gov

Payment Error Prevention Program (PEPP)

In 1997, the Office of Inspector General (OIG) of Health and Human Services (HHS) reported that approximately $4 billion in improper Medicare payments were made for inpatient services under the diagnosis related group (DRG) prospective payment system (PPS). The **Payment Error Prevention Program (PEPP)** was initiated, and requires facilities to identify and reduce improper Medicare payments and, specifically, the Medicare payment error rate. (CMS defines the **payment error rate** as the number of dollars found to be paid in error out of the total of all dollars paid for inpatient PPS services.) CMS determines the inpatient payment error rate for each state, and facility performance is evaluated in part on the basis of reductions in this payment error rate. **Clinical Data Abstraction Centers (CDACs)** were established and became responsible for initially requesting and screening medical records for the PEPP surveillance sample for medical review, DRG validation, and medical necessity. Medical review criteria applied by the CDACs to screen medical records were developed by Peer Review Organizations (PROs), now called Quality Improvement Organizations (QIOs).

Overpayment Recovery

Overpayments are funds a provider or beneficiary has received in excess of amounts due and payable under Medicare and Medicaid statutes and regulations. Once a determination of overpayment has been made, the amount so determined is a debt owed to the United States Government. The **Federal Claims Collection Act of 1966** requires carriers and fiscal intermediaries (as agents of the federal government) to attempt the collection of overpayments. Examples of overpayments include:

- payment based on a charge that exceeds the reasonable charge.
- duplicate processing of charges/claims.
- payment to a physician on a nonassigned claim or to a beneficiary on an assigned claim. (Payment made to wrong payee.)
- payment for noncovered items and services, including medically unnecessary services.
- incorrect application of the deductible or coinsurance.
- payment for items or services rendered during a period of nonentitlement.
- primary payment for items or services for which another entity is the primary payer.
- payment for items or services rendered after the beneficiary's date of death. (Post-payment reviews are conducted to identify and recover payments with a billed date of service that is after the beneficiary's date of death.)

When a carrier or fiscal intermediary determines that an overpayment was made, it proceeds with recovery by issuing an overpayment demand letter (Figure 5-10) to the provider. The letter contains information about the review and statistical sampling methodology used as well as corrective actions to be taken. (An explanation of the sampling methodology that was followed is included.) Corrective actions include payment suspension, imposition of civil money penalties, institution of pre- or post-payment review, additional edits, and so on.

Providers and beneficiaries can receive a waiver of recovery of overpayments if one or more of the following provisions apply:

- Overpayment was discovered subsequent to the third calendar year after the year of payment.
- If an overpaid physician is found to be without fault or is deemed without fault, overpayment shifts to the beneficiary (e.g., medically unnecessary services).
- When both provider and beneficiary are without fault with respect to an overpayment on an assigned claim for medically unnecessary services, liability is waived for the overpayment (e.g., no action taken to recover the overpayment).
- If a beneficiary is liable for an incorrect payment, CMS or SSA may waive recovery if the beneficiary was without fault with respect to the overpayment and recovery would cause financial hardship or would be against equity and good conscience.

Carriers and fiscal intermediaries are prohibited from seeking overpayment recovery when the following two time limitations apply:

- Overpayment is not reopened within four years (48 months) after the date of payment, unless the case involves fraud or similar fault.

(Insert Medicare carrier letterhead here)

May 15, YYYY

Doug M. Smith, M.D.
393 Main St
Anywhere US 12345

RE:	EMPLOYEE:	**Nathan A. Sanders**	CLAIM #:	**939395SLD0005**
	SSN:	**123-45-6789**	GROUP #:	**02365**
	PATIENT:	**Nathan A. Sanders**	DIV DESC:	**PRODUCTION MAIL**
	EMPLOYER:	**Global Center**	LOC DESC:	**NY**

Dear Provider:

Please be advised that an overpayment of benefits has been made for the above named patient. In order to resolve this matter we are asking you to make reimbursement. Please make your check payable to:

GLOBAL CARE MEDICAL CENTER

in the amount of

$675.00

and forward it to:

EMPIRE STATE HEALTH PLAN
P.O. BOX 93902
ANYWHERE US 12345

We are requesting this refund due to the following reason:

CLAIM WAS PROCESSED UNDER THE WRONG PATIENT FOR DATES OF SERVICE 4/15 & 4/20/YYYY.

If you have any questions, please feel free to contact us.

Sincerely,

Mary Louise Smith
Claims Analyst (39-392)

FIGURE 5-10 Sample overpayment letter

- Overpayment is discovered later than three full calendar years after the year of payment unless there is evidence that the provider or beneficiary was at fault with respect to the overpayment.

Provider Liability for Overpayments

Providers are liable for refunding an overpayment in the following situations:

- Overpayment resulted from incorrect reasonable charge determination (because providers are responsible for knowing Medicare reasonable charges for services).

  Exception: If the provider's reasonable charge screen was increased and the physician had no reason to question the amount of the increase, the physician is not liable and the case is referred to CMS for review.

NOTE: If the provider has reason to believe the increase was excessive, the provider is liable unless the question was brought promptly to the attention of the carrier or fiscal intermediary who assured the physician that the increase was correct.

- Provider received duplicate payments from the carrier or fiscal intermediary (because the claim was processed more than once, or the provider submitted duplicate claims).

NOTE: The provider does not have a reasonable basis for assuming that the total payment received was correct and thus should have questioned it. The provider is, therefore, at fault and liable for the overpayment.

- Provider received payment on the basis of **assignment** (the provider agreed to accept as payment whatever the payer deemed a reasonable charge), and a beneficiary received payment on an itemized bill and submitted that payment to the provider.

NOTE: The provider is liable for the portion of the total amount paid in excess of the reasonable charge (including any copayment paid by the beneficiary). The beneficiary is liable for the balance of the overpayment. If the provider protests recovery of the overpayment on the grounds that all or part of the check received from the beneficiary was applied to amounts the beneficiary owed for other services, the beneficiary, rather than the physician, is liable for refunding such amounts.

EXAMPLE: Mary Sue Patient underwent office surgery on May 15 performed by Dr. Smith. Medicare determined the reasonable charge for the office surgery to be $375. In July, Dr. Smith and Mary Sue Patient each received a check from Medicare in the amount of $300. Mary Sue Patient then signed her $300 over to Dr. Smith. Thus, Dr. Smith received a total of $600 for services provided on May 15, an overpayment of $225 (the amount received in excess of the reasonable charge). Mary Sue Patient is liable for the remaining $75 of the duplicate payment. (If Mary Sue Patient had also previously paid Dr. Smith the $75 as coinsurance, Dr. Smith would be liable for the entire $300 overpayment.) *Dr. Smith is responsible for contacting the Medicare carrier to report the overpayment and make arrangements to provide a refund to the carrier.*

- Provider received duplicate payments from Medicare and another payer directly or through the beneficiary, which happens to be the primary payer (e.g., automobile medical or no-fault insurer, liability insurer, or workers' compensation).

NOTE: The provider is liable for the portion of the Medicare payment in excess of the amount Medicare is obligated to pay as a secondary payer. However, if the provider signs the other insurance payment over to the beneficiary, the beneficiary is liable.

- Provider was paid but does not accept assignment.

NOTE: The provider is liable whether or not the beneficiary had also been paid.

- Provider furnished erroneous information, or provider failed to disclose facts known or that should have been known and that were material to payment of benefit.

  EXAMPLE 1: A beneficiary is referred to a provider by an employer for a fracture that occurred during a fall at work. The physician billed Medicare and neglected to indicate on the claim that the injury was work-related (although that information had been provided by the patient). If Medicare benefits are paid to the provider for services and the injury would have been covered by workers' compensation, the provider is liable for an overpayment because of failure to disclose that the injury was work-related.

  EXAMPLE 2: A provider submitted an assigned claim showing total charges of $1,000. The provider did not indicate on the claim that any portion of the bill had been paid by the patient. The carrier determined the reasonable charge to be $600 and paid the physician $480 (80% of $600) on the assumption that no other payment had been received. The carrier later learned that the beneficiary had paid the physician $200 before the provider submitted his claim. Thus, the payment should have been split between provider and beneficiary with $400 paid to the provider and $80 to the beneficiary. The provider is liable for causing the $80 overpayment as the amount received from the beneficiary was not reported on the claim. ●

- Provider submitted a claim for services other than medically unnecessary services, but should have known they would not be covered (e.g., conversation with a relative of a beneficiary).

  NOTE: Generally, allegations by a provider as not liable for payments received for noncovered services because provider was unaware of coverage provisions is not a basis for finding the provider without fault.

- Provider submitted a claim for medically unnecessary services.

  NOTE: In these matters, criteria for determining whether the provider knew or should have known that services were not covered are followed by carriers and fiscal intermediaries. ●

- Items or services were furnished by provider or supplier not qualified for Medicare reimbursement.

  EXAMPLE 1: A lab test is performed by a nonqualified independent laboratory.

  EXAMPLE 2: Services are rendered by a naturopath. ●

- Overpayment was due to a mathematical or clerical error.

  NOTE: The failure to properly assess the deductible is not considered a mathematical error. ●

- Provider does not submit documentation to substantiate services billed or where there is question as to whether services were actually performed (e.g., fraud is suspected).

- Overpayment was for rental of durable medical equipment, and supplier billed under the one-time authorization procedure.

NOTE: Suppliers of durable medical equipment who have accepted assignment may be reimbursed for rental items on the basis of a one-time authorization by the beneficiary (e.g., without the need to obtain beneficiary's signature each month). A supplier using the procedure must have filed with the carrier a statement that it assumes unconditional responsibility for rental overpayments for periods after the beneficiary's death or while beneficiary was institutionalized or no longer needed or used the equipment.

Absence of Provider Liability for Overpayments

A provider is liable for overpayments received unless found to be *without fault* as determined by the carrier or fiscal intermediary. A provider can be considered without fault if reasonable care was exercised in billing for and accepting payment, and the provider had a reasonable basis for assuming that payment was correct. In addition, if the provider had reason to question the payment and promptly brought the question to the attention of the carrier or fiscal intermediary, he may be found without liability.

NOTE: The provider must make full disclosure to the carrier or fiscal intermediary of all material facts and the basis on which information was made available, including, but not limited to, Medicare regulations.

The above criteria are always met in the case of overpayments due to an error with respect to the beneficiary's entitlement to Medicare benefits and the carrier's or fiscal intermediary's failure to properly apply the deductible. Normally, it is clear from the circumstances of the overpayment whether the provider was without fault in causing the overpayment. When this is not clear from the record, the carrier or fiscal intermediary must review the issue (as long as the review occurs within three calendar years after the year in which the overpayment was made).

Correct Coding Initiative

The Centers for Medicare and Medicaid Services (CMS) developed the National *Correct Coding Initiative (CCI)* in 1996 to reduce Medicare program expenditures by detecting inappropriate codes submitted on claims and denying payment for them, promoting national correct coding methodologies, and eliminating improper coding practices. (Table 5-1 contains a list of CCI terms, definitions and examples.) There are over 140,000 CCI **code pairs** (or **edit pairs**) that cannot be reported on the same claim, and they are based on coding conventions defined in CPT, current standards of medical and surgical coding practice, input from specialty societies, and analysis of current coding practices. CMS contracts with AdminaStar Federal, Inc., an Indiana Medicare carrier, to develop and maintain coding edits, which are published by the National Technical Information Service (NTIS).

INTERNET LINKS

CCI Edits Manual from NTIS	http://www.ntis.gov
AdminaStar Federal, Inc.	http://www.adminastar.com
Medicare's National CCI Edits	http://www.cms.hhs.gov/medlearn/ncci.asp

TABLE 5-1 Medicare's National CCI terms and definitions

TERM	DEFINITION	EXAMPLE
CCI Edits	Pairs of CPT and/or HCPCS level II codes, which are not separately payable except under certain circumstances (e.g., reporting appropriate modifier). The edits are applied to services billed by the same provider for the same beneficiary on the same date of service.	The surgeons intends to perform laparoscopic cholecystectomy; upon visualization of the gallbladder, it is determined than an open cholecystectomy is required. If the surgeon reports CPT codes for removal of an organ through an open incision as well as with laparoscopy, the CCI edit results in claims denial. **NOTE:** If a laparoscopic procedure becomes an open procedure, report only the open procedure code. ●
Comprehensive Code	The major procedure or service when reported with another code. The *comprehensive code* represents greater work, effort, and time as compared to the other code reported. (Also called "column 1 codes.") Higher payments are associated with comprehensive codes.	The patient undergoes deep biopsy as well as superficial biopsy of the same site. If the surgeon reports CPT codes for the deep and superficial biopsy, the CCI edit results in claims denial. **NOTE:** Report only the deep biopsy when both deep and superficial biopsies are performed at the same location. ● If the surgeon determines that the superficial biopsy code should be reported in addition to the deep biopsy code, supporting documentation in the patient's record must be evident. **NOTE:** A modifier must be added to the code. A **modifier** is a two-digit code added to the main code to indicate a procedure/service has been altered (e.g., bilateral procedure). ●
Component Code	The lesser procedure or service when reported with another code. The *component code* is part of a major procedure or service, and is often represented by a lower work relative value unit (RVU) under the Medicare Physician Fee Schedule as compared to the other code reported. (Also called *column 2 codes*.) Lower payments are associated with component codes.	
Comprehensive/ Component Edit Table (Figure 5-11	Code combinations (or edit pairs), where one of the codes is a component of the more comprehensive code and only the comprehensive code is paid. (If clinical circumstances justify appending a CCI associated modifier to either code of a code pair edit, payment of both codes may be allowed.)	Figure 5-11 contains a partial listing of comprehensive/component codes. Refer to Column 1 code 10140. If code 10140 is reported on a CMS-1500 claim, none of the codes from Column 2 can be reported on the same claim (unless a modifier is attached and supporting documentation is found in the patient's record).

(continues)

TABLE 5-1 *(continued)*

TERM	DEFINITION	EXAMPLE
Mutually Exclusive Codes	Procedures or services that could not reasonably be performed at the same session by the same provider on the same beneficiary.	A claim that contains codes for cystourethroscopy, with internal urethrotomy of a female (CPT code 52270) with that of a male (CPT code 52275) will result in denial as a result of this CCI edit.
Mutually Exclusive Edit Table (Figure 5-12)	Code combinations (or edit pairs), where one of the procedures/services would not reasonably be performed with the other. (If clinical circumstances justify adding a CCI modifier to either code of a code pair edit, payment of both codes may be allowed.)	Figure 5-12 contains a partial listing of mutually exclusive codes. Refer to Column 1 code 10060. If code 10060 is reported on a CMS-1500 claim, none of the codes from Column 2 can be reported on the same claim (unless a modifier is attached and supporting documentation is found in the patient's record).

CORRECT CODING EDITS FOR COMPREHENSIVE CODES 10000-19999 CPT codes only © Copyright AMA

Comprehensive	Component	Comprehensive	Component
10021	19290	10140	11055, 11056, 11057, 11719,
10022	10021, 19290		11720, 11721, 69990, G0127
10040	69990	10160	11055, 11056, 11057, 11719,
10060	11055, 11056, 11057, 11719,		11720, 11721, 69990, G0127

FIGURE 5-11 Partial listing of Correct Coding Edits for Comprehensive/Component Code Edits (This figure is for illustrative purposes only and may not represent current version published in NTIS manual.)

CORRECT CODING EDITS FOR MUTUALLY EXCLUSIVE CODES 10000-19999 CPT codes only © Copyright AMA

Column 1	Column 2	Column 1	Column 2
10060	11401, 11402, 11403, 11404,	10160	10061, 10140
	11406, 11421, 11422, 11423,	11000	11010, 11011, 11012, 11056,
	11424, 11426, 11441, 11442,		11057, 15000, 97601
	11443, 11444, 11446, 11450,	11010	20150, 20561, 20662, 20663

FIGURE 5-12 Partial Listing of Mutually Exclusive Correct Coding Edits (This figure is for illustrative purposes only and may not represent current version published in NTIS manual.)

INTERNET LINKS

CCI edits are also available as part of vendor encoder software, including the CodeCorrect.com online product at http://www.codecorrect.com, which is updated as new versions of CCI edits become available.

EncoderPro software from Ingenix includes CCI unbundling edits. Go to http://www.ingenixonline.com and click on Software for more information.

NOTE: Under a previous CMS contract, a private company refused to publish code edits they developed because they considered them proprietary; these nonpublished code edits were called **black box edits**. Use of these edits was discontinued when CMS did not renew its contract with the company, and future CMS contracts do not allow for such restrictions.

Medical Savings Accounts

HIPAA permits eligible individuals to establish a *medical savings account (MSA)*, a tax-exempt trust or custodial account established for the purpose of paying medical expenses in conjunction with a high-deductible health plan. Individuals eligible to establish an MSA include:

- an employee (or spouse of an employee) of a "small employer" that maintains an individual or family "high-deductible health plan" covering that individual (employee or spouse), or
- a self-employed person (or spouse of self-employed person) that maintains an individual or family "high-deductible health plan" covering that individual (self-employed person or spouse).

Access to Long-Term Care Services

HIPAA contains tax clarification provisions for long-term care insurance to assure that the tax treatment for private long-term care insurance is the same as for major medical coverage. Insurance companies must also follow certain administrative and marketing practices or face significant fines.

EXAMPLE 1: Consumers must be provided with a description of the policy's benefits and limitations before making a commitment to allow consumers to compare policies from different companies.

EXAMPLE 2: Companies must report annually the number of claims denied, information on policy replacement sales, and policy terminations data.

No policy can be sold as a long-term care insurance policy if it limits or excludes coverage by type of treatment, medical condition, or accident. An exception to this rule, however, includes policies that may limit or exclude coverage for pre-existing conditions or diseases, mental or nervous disorders (but not Alzheimer's), or alcoholism or drug addiction. The law also prohibits a company from canceling a policy except for nonpayment of premiums.

Administrative Simplification

HIPAA was part of a Congressional attempt at incremental health care reform, with the *Administrative Simplification* aspect requiring DHHS to develop standards for maintenance and transmission of health information required to identify individual patients. These standards are designed to:

- improve efficiency and effectiveness of the health care system by standardizing the interchange of electronic data for specified administrative and financial transactions.
- protect the security and confidentiality of electronic health information.

The requirements outlined by law and the regulations implemented by DHHS require compliance by *all* health care organizations that maintain or transmit electronic health information (e.g., health plans; health care clearinghouses; and health care providers, from large integrated delivery networks to individual physician offices).

The law also provides for significant financial penalties for violations.

General penalty for failure to comply:

- each violation: $100
- maximum penalty for all violations of an identical requirement: may not exceed $25,000

Wrongful disclosure of individually identifiable health information:

- wrongful disclosure offense: $50,000; imprisonment of not more than one year; or both
- offense under false pretenses: $100,000; imprisonment of not more than 5 years; or both
- offense with intent to sell information: $250,000; imprisonment of not more than 10 years; or both.

Unique Identifiers

The administrative simplification (AS) provision of HIPAA requires establishment of standard identifiers for third-party payers (e.g., insurance companies, Medicare, and Medicaid), providers, and employers, as follows:

- **National Health PlanID (PlanID)** (formerly called PAYERID) will be assigned to third-party payers; it is expected to have ten numeric positions, including a check digit as the tenth position. (A **check digit** is a one-digit character, alphabetic or numeric, which is used to verify the validity of a unique identifier.)
- **National Individual Identifier** (patient identifier) has been put on hold. Several bills in Congress would eliminate the requirement to establish a National Individual Identifier.

  NOTE: California implemented a regulation that prohibits the use of social security numbers on health plan ID cards and health-related correspondence.

- **National Provider Identifier (NPI)** will be assigned to health care providers as an 8- or possibly 10-character alphanumeric identifier, including a check digit in the last position.

- **National Standard Employer Identifier Number (EIN)** is assigned to employers who, as sponsors of health insurance for their employees, need to be identified in health care transactions. It is the federal employer identification number (EIN) assigned by the Internal Revenue Service (IRS) and has nine digits with a hyphen (00-0000000). EIN assignment by the IRS began in January 1998.

Electronic Health Care Transactions

HIPAA requires payers to implement **electronic transaction standards** (or transactions rule), which is a uniform language for electronic data interchange. **Electronic data interchange (EDI)** is the process of sending data from one party to another using computer linkages. The CMS Standard EDI Enrollment Form must be completed prior to submitting electronic media claims (EMC) to Medicare. The agreement must be executed by each provider of health care services, physician, or supplier that intends to submit EMC.

EXAMPLE: Health care providers submit electronic claims data to payers on computer tape, diskette, or by computer modem or fax. The payer receives the claim, processes the data, and sends the provider the results of processing electronic claims (an electronic transmittal notice). ●

NOTE: Computer-generated paper claims are not categorized as EDI. ●

The final rule on transactions and code sets was effective October 16, 2002 for large plans and October 16, 2003 for small plans. It requires the following to be used by health plans, health care **clearinghouses** (which perform centralized claims processing for providers and health plans), and health care providers who participate in electronic data interchanges:

- Three electronic formats are supported for health care claim transactions, including the UB-92 flat-file format, the National Standard Format (NSF), and the ANSI ASC X12 837 (American National Standards Institute (ANSI), Accredited Standards Committee (ASC), Insurance Subcommittee (X12N), Claims validation tables (837).

  NOTE: A **flat file** consists of a series of fixed-length records (e.g., 25 spaces for patient's name). The **UB-92** flat file is used to bill institutional services, such as services performed in hospitals. The **National Standard Format (NSF)** flat file format is used to bill physician and noninstitutional services, such as services reported by a general practitioner on a CMS-1500 claim. The **ANSI ASC X12 837** variable-length file format is used to bill institutional, professional, dental, and drug claims. ●
- Dental services are using *Current Dental Terminology* (CDT) codes. ***Current Dental Terminology* (CDT)** is a medical code set that is maintained and copyrighted by the American Dental Association.
- Diagnoses and inpatient hospital services are reported using *International Classification of Diseases, 9th Revision, Clinical Modification* (ICD-9-CM) codes.

  NOTE: This will change to ICD-10-CM when adopted for implementation (possibly 2005). ●

- Physician services are reported using *Current Procedural Terminology* (CPT) codes.
- Procedures are reported using: ICD-9-CM (Index to Procedures and Tabular List of Procedures) and the *Healthcare Common Procedure Coding System* (HCPCS), *Level I* (CPT) and *Level II (national)* codes.
- Institutional and professional pharmacy transactions are reported using HCPCS, *Level II (national)* codes.
- Retail pharmacy transactions are reported using the *National Drug Code* (NDC) manual.

The ***National Drug Code* (NDC)** is maintained by the Food and Drug Administration (FDA) and identifies prescription drugs and some over the counter products. Each drug product is assigned a unique 11-digit, 3-segment number, which identifies the vendor, product, and trade package size.

INTERNET LINKS

ANSI ASC X12N 837 implementation guides are available at http://www.wpc-edi.com

Retail pharmacy standards implementation guide is available at http://www.ncpdp.org

Go to http://cms.hhs.gov and click the Medicare link, and then the Electronic Data Interchange (EDI) link to download the CMS Standard EDI Enrollment Form.

Privacy Standards

HHS published the final Privacy Rule on December 28, 2000, and the final rule took effect on April 14, 2001. The **Privacy Rule** creates national standards to protect individuals' medical records and other personal health information. This rule also gives patients greater access to their own medical records and more control over how their personal health information is used. The rule addresses the obligations of health care providers and health plans to protect health information. By law, covered entities (health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically) have until April 14, 2003, to comply. (Small health plans have until April 14, 2004, to comply.) The HHS Office for Civil Rights (OCR) has implementation and enforcement responsibility for the Privacy Rule.

NOTE: Covered entities are bound by the Privacy Rule even if they contract with business associates to perform some of their essential functions. A **business associate** is a person or entity that provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of protected health information (PHI).

On July 6, 2001, OCR issued the first in a series of guidance materials that answer some of the questions about the new protections for consumers and requirements for doctors, hospitals, other providers, health plans and health insurers, and health care clearinghouses. It also clarifies some of the confusion regarding the meaning of key provisions of the rule. Final modifications to the Privacy Rule were published in the August 14, 2002 *Federal Register*, and a new subpart was added—*Subpart E: Privacy of Individually Identifiable Health Information*. The Privacy Rule requires the implementation of activities, such as:

- providing information to patients about their privacy rights and how their information can be used.
- adopting clear privacy procedures for its practice, hospital, or plan.
- training employees so they understand the privacy procedures.
- designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

To ease the burden of complying with the new requirements, the Privacy Rule incorporates flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. For example:

- The privacy official at a small physician practice may be the office manager, who will have other nonprivacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies, whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
- The policies and procedures of small providers may be more limited under the rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

INTERNET LINKS

Guidance materials can be found at http://aspe.hhs.gov by clicking on the *Administrative Simplification in the Health Care Industry (HIPAA)* link

The HHS Office for Civil Rights provides information on the new regulation at http://www.hhs.gov/ocr/hipaa

Sample business associate contract provisions can be found at http://www.hhs.gov/ocr/hipaa/contractprov.html

NOTE: Patient access to personal information in CMS's records is also governed by the *Privacy Act of 1974,* which protects Federal records that can be retrieved by a personal identifier.

NOTE: The Privacy Rule does not preempt state laws that are more restrictive than federal regulations.

HHS recognizes that the privacy standards are restrictive, and the following revisions are under consideration:

- *Phoned-in Prescriptions:* Pharmacists will be permitted to continue filling prescriptions phoned in by a patient's doctor before obtaining the patient's written consent.

- *Referral Appointments:* Direct treatment providers receiving a first time patient referral will be permitted to schedule appointments, surgery, or other procedures before obtaining the patient's signed consent. A **direct treatment provider** is one who treats a patient directly, rather than based on the orders of another provider, and/or provides health care services or test results directly to patients.
- *Allowable Communications:* Covered entities will be free to engage in whatever communications are required for quick, effective, high quality health care, including routine oral communications with family members, treatment discussions with staff involved in coordination of patient care, and using patient names to locate them in waiting areas.
- *Minimum Necessary Scope:* Certain common practices, such as the use of sign-up sheets and X-ray lightboards, and maintenance of patient medical charts at the bedside are allowed under the rule.
- *Parents and Minors:* Parents will continue to have appropriate access to information about the health and well-being of their children.

The Privacy Rule establishes a federal requirement that doctors, hospitals, or other health care providers obtain a patient's written consent and an authorization before using or disclosing the patient's protected health information (PHI) to carry out *treatment, payment, or health care operations (TPO).* A **consent** is a general document that gives health care providers, who have a direct treatment relationship with a patient, permission to use and disclose all PHI for TPO. It gives permission only to that provider, not to any other person, and one consent covers all uses and disclosures for TPO by that provider indefinitely.) The Privacy Rule establishes a uniform standard for certain health care providers to obtain their patients' consent for uses and disclosures of health information about the patient to carry out TPO. An **authorization** is a customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. It covers only the uses and disclosures and only the PHI stipulated in the authorization; it has an expiration date; and, in some cases, it also states the purpose for which the information may be used or disclosed. The Privacy Rule also requires that "reasonable steps" be taken to ensure that patient records are secured at all times (e.g., storing records in locked cabinets to prevent unauthorized access).

NOTE: Privacy violations are subject to no more than $100 per person per violation not to exceed $25,000 per person per year per violation of a single standard. More serious violations are subject to more severe penalties, including:

- $50,000 and/or up to one year in prison for persons who knowingly obtain and disclose protected health information.
- $100,000 and/or up to five years in prison for persons who under "false pretense" obtain and disclose protected health information.
- $250,000 and up to 10 years in prison for persons with intent to sell, transfer, or use for malicious reasons or personal gain, protected health information.

SUMMARY

- Federal and state statutes are laws passed by legislative bodies, which are implemented as regulations (guidelines written by administrative agencies).
- Case law (or common law) is based on court decisions that establish a precedent (or standard).
- The *Federal Register* is a legal newspaper published every business day by the federal government.
- The *Medicare Bulletin* serves as a legal notice to providers about Medicare laws, regulations, and guidelines.
- A Medicare carrier contracts with CMS to process Medicare Part B claims, and a fiscal intermediary processes Medicare Part A claims.
- A listserv is a subscriber-based question-and-answer forum that is available through e-mail.
- Patient health care information must be maintained in a confidential and secure manner. Confidentiality restricts access to patient information (a patient authorization is required to release information). Privacy is the right of individuals to keep information from being disclosed to others. Security involves the safekeeping of patient information. Breach of confidentiality is the unauthorized release of information to a third party.
- A contract is an agreement between two or more parties to perform specific services or duties. A verbal contract is established between patient and provider when the patients seeks medical services.
- Patients must sign the "Authorization for Release of Medical Information" located in Block 12 of the CMS-1500 claim or sign a special release form that is maintained by the practice. (Enter SIGNATURE ON FILE in Block 12 of the CMS-1500 claim.)
- Special rules apply to the release of HIV/AIDS, drug/alcohol, and mental health information.
- Do not release information over the telephone unless you have verified that the person making the request is entitled to the information.
- Limit the submission of faxed information to that required to satisfy the immediate needs of the requesting party or to assist emergency health care situations.
- Sensitive information submitted via the Internet must be encrypted (converted to a secure language for transmission).
- Patient information and health insurance records must be maintained for a minimum of six years unless state law specifies a longer period.
- The Federal False Claims Act regulates fraudulent practices, such as upcoding (assigning an ICD-9-CM diagnosis code that does not match documentation to increase inpatient reimbursement).
- Stark II regulations legislate self-referrals by providers who order services to be performed for patients at a facility in which they have a financial interest.
- ERISA ensures that pension and other benefits are provided to employees as promised by their employers, and COBRA includes provisions for continuation of health care coverage if employment is discontinued due to a triggering event (e.g., layoff).

- Medical necessity is the measure of whether a health care procedure or service will be reimbursed by a payer. It is usually based on the recommendations of the provider and the payer's representative.
- HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996, which includes many provisions: health insurance reform, administrative simplification, fraud and abuse guidelines, use of medical savings accounts, improved access to long-term care services and coverage, electronic health information transaction standards, and privacy and security standards for health information.
- The Payment Error Prevention Program (PEPP) identifies and reduces improper Medicare payments and the payment error rate. Overpayment recovery involves the collection of overpayments made to health care provided by Medicare, Medicaid, and other payers.
- The Correct Coding Initiative (CCI) was implemented to reduce Medicare program expenditures by detecting inappropriate coding on claims and denying payment for them.

STUDY CHECKLIST

- ❒ Read the textbook chapter and highlight key concepts.
- ❒ Create an index card for each key term.
- ❒ Access the chapter Internet links to learn more about concepts.
- ❒ Answer the chapter review questions, verifying answers with your instructor.
- ❒ Complete Web Tutor assignments and take online quizzes.
- ❒ Complete Workbook chapter, verifying answers with your instructor.
- ❒ Form a study group with classmates to discuss chapter concepts in preparation for an exam.

REVIEW

TRUE/FALSE

Indicate whether each statement is true or false.

1. ☐ T ☐ F Breach of confidentiality is the release of confidential patient information to a third party.
2. ☐ T ☐ F Fraud is the deception or misrepresentation made by an individual, knowing it to be false, which could result in some unauthorized benefit.
3. ☐ T ☐ F A contract is an agreement between two or more parties to perform specific services or duties.
4. ☐ T ☐ F A patient/provider contract for medical services is negotiated so that the payer will agree to promptly pay the physician's usual fee for services performed.
5. ☐ T ☐ F A guardian is a person who has legal responsibility for a minor child or incompetent adult.

SHORT ANSWER

Briefly respond to each of the following.

6. Identify the problem in each case scenario that results in a breach of confidentiality.
   a. An insurance company sends a letter on company letterhead requesting a copy of a patient's records in order to process payment. No other documents accompany the letter.
   b. An attorney calls the office and requests that a copy of his client's medical record be immediately faxed to the attorney's office.
   c. An insurance company calls the office to request information about a claim. Dates of service are confirmed as well as the patient's HIV status.
   d. Diagnostic and treatment data about a competent adult is requested by the patient's spouse.
   e. Case studies about patients are discussed in the classroom.
7. Explain how a health insurance specialist could unwittingly be involved in committing fraud by interacting with the following individuals:
   a. health care provider
   b. patient
   c. widow/widower of a deceased patient
8. List the monetary and/or prison term penalties for committing Medicare fraud.
9. Identify the overpayment amount for the following cases along with the liable party.
   a. Patient received services on April 5, totaling $1,000. The provider accepted assignment, and the payer established the reasonable charge as $450. On July 1, the provider received $360 from the insurance company, representing an 80% payment of the reasonable charge. The patient had paid a $90 coinsurance at the time of the visit. On August 1, the patient received a check from the insurance company in the amount of $450.
   b. Patient underwent office surgery on October 10, and Medicare determined the reasonable charge to be $650. The provider and patient each received a check for $500, and the patient signed the check over to the provider. The patient had not paid a coinsurance at the time of the office surgery.
   c. Patient was treated in the Emergency Department for a fractured arm. The chief complaint was "I was moving a file cabinet for my boss when it tipped over and fell on my arm." The facility billed the patient's employer group insurance policy and received reimbursement of $550.
   d. The provider submitted an assigned claim for which the payer determined the reasonable charge was $500. The payer reimbursed the provider $400 (80% of the reasonable charge). It was later determined that the patient had paid $200 at the time of the visit.
10. Identify the monetary and/or prison term penalties established by HIPAA for breaching a patient's protected health information.