HIPAA Privacy and Security

HOW TO RECEIVE CREDIT

- Read the enclosed course.
- Complete the questions at the end of the course.
- Return your completed Evaluation to NetCE by mail or fax, or complete online at www.NetCE.com. (If you are a physician, behavioral health professional, or Florida nurse, please return the included Answer Sheet/Evaluation.) Your postmark or facsimile date will be used as your completion date.
- Receive your Certificate(s) of Completion by mail, fax, or email.

Faculty
Carol Shenold, RN, ICP, graduated from St. Paul's Nursing School, Dallas, Texas, achieving her diploma in nursing. Over the past thirty years she has worked in hospital nursing in various states in the areas of obstetrics, orthopedics, intensive care, surgery and general medicine.

Mrs. Shenold served as the Continuum of Care Manager for Vencor Oklahoma City, coordinating quality review, utilization review, Case Management, Infection Control, and Quality Management. During that time, the hospital achieved Accreditation with Commendation with the Joint Commission, with a score of 100.

Mrs. Shenold was previously the Infection Control Nurse for Deaconess Hospital, a 300-bed acute care facility in Oklahoma City. She is an active member of the Association for Professionals in Infection Control and Epidemiology (APIC). She worked for the Oklahoma Foundation for Medical Quality for six years.

Faculty Disclosure
Contributing faculty, Carol Shenold, RN, ICP, has disclosed no relevant financial relationship with any product manufacturer or service provider mentioned.

Division Planners
Ronald Runciman, MD
Jane C. Norman, RN, MSN, CNE, PhD
Alice Yick Flanagan, PhD, MSW
James Trent, PhD

Director of Development and Academic Affairs
Sarah Campbell

Division Planners/Director Disclosure
The division planners and director have disclosed no relevant financial relationship with any product manufacturer or service provider mentioned.

Audience
This course is designed for all members of the interprofessional healthcare team.

Accreditations & Approvals
In support of improving patient care, NetCE is jointly accredited by the Accreditation Council for Continuing Medical Education (ACCME), the Accreditation Council for Pharmacy Education (ACPE), and the American Nurses Credentialing Center (ANCC), to provide continuing education for the healthcare team.

As a Jointly Accredited Organization, NetCE is approved to offer social work continuing education by the Association of Social Work Boards (ASWB) Approved Continuing Education (ACE) program. Organizations, not individual courses, are approved under this program. State and provincial regulatory boards have the final authority to determine whether an individual course may be accepted for continuing education credit. NetCE maintains responsibility for this course.

NetCE has been approved by NBCC as an Approved Continuing Education Provider, ACEP No. 6361. Programs that do not qualify for NBCC credit are clearly identified. NetCE is solely responsible for all aspects of the programs.

Designations of Credit
NetCE designates this enduring material for a maximum of 5 *AMA PRA Category 1 Credit(s)*™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Successful completion of this CME activity, which includes participation in the evaluation component, enables the participant to earn up to 5 MOC points in the American Board of Internal Medicine's (ABIM) Maintenance of Certification (MOC) program. Participants will earn MOC points equivalent to the amount of CME credits claimed for the activity. It is the CME activity provider's responsibility to submit participant completion information to ACCME for the purpose of granting ABIM MOC credit. Completion of this course constitutes permission to share the completion data with ACCME.

Successful completion of this CME activity, which includes participation in the evaluation component, enables the learner to earn credit toward the CME and Self-Assessment requirements of the American Board of Surgery's Continuous Certification program. It is the CME activity provider's responsibility to submit learner completion information to ACCME for the purpose of granting ABS credit.

Copyright © 2022 NetCE

A complete Works Cited list begins on page 24.

Mention of commercial products does not indicate endorsement.

This activity has been approved for the American Board of Anesthesiology's® (ABA) requirements for Part II: Lifelong Learning and Self-Assessment of the American Board of Anesthesiology's (ABA) redesigned Maintenance of Certification in Anesthesiology Program® (MOCA®), known as MOCA 2.0®. Please consult the ABA website, www.theABA.org, for a list of all MOCA 2.0 requirements. Maintenance of Certification in Anesthesiology Program® and MOCA® are registered certification marks of the American Board of Anesthesiology®. MOCA 2.0® is a trademark of the American Board of Anesthesiology®.

Successful completion of this CME activity, which includes participation in the activity with individual assessments of the participant and feedback to the participant, enables the participant to earn 5 MOC points in the American Board of Pediatrics' (ABP) Maintenance of Certification (MOC) program. It is the CME activity provider's responsibility to submit participant completion information to ACCME for the purpose of granting ABP MOC credit.

This activity has been designated for 5 Lifelong Learning (Part II) credits for the American Board of Pathology Continuing Certification Program.

Successful completion of this CME activity, which includes participation in the evaluation component, earns credit toward the Lifelong Learning requirement(s) for the American Board of Ophthalmology's Continuing Certification program. It is the CME activity provider's responsibility to submit learner completion information to ACCME for the purpose of granting credit.

Through an agreement between the Accreditation Council for Continuing Medical Education and the Royal College of Physicians and Surgeons of Canada, medical practitioners participating in the Royal College MOC Program may record completion of accredited activities registered under the ACCME's "CME in Support of MOC" program in Section 3 of the Royal College's MOC Program.

NetCE designates this continuing education activity for 5 ANCC contact hours.

IPCE CREDIT™

This activity was planned by and for the healthcare team, and learners will receive 5 Interprofessional Continuing Education (IPCE) credits for learning and change.

NetCE designates this continuing education activity for 6 hours for Alabama nurses.

AACN Synergy CERP Category B.

Social Workers participating in this intermediate to advanced course will receive 5 Clinical continuing education clock hours.

NetCE designates this continuing education activity for 2 NBCC clock hours.

Individual State Nursing Approvals

In addition to states that accept ANCC, NetCE is approved as a provider of continuing education in nursing by: Alabama, Provider #ABNP0353 (valid through 07/29/2025); Arkansas, Provider #50-2405; California, BRN Provider #CEP9784; California, LVN Provider #V10662; California, PT Provider #V10842; District of Columbia, Provider #50-2405; Florida, Provider #50-2405; Georgia, Provider #50-2405; Kentucky, Provider #7-0054 (valid through 12/31/2023); South Carolina, Provider #50-2405; West Virginia, RN and APRN Provider #50-2405.

Individual State Behavioral Health Approvals

In addition to states that accept ASWB, NetCE is approved as a provider of continuing education by the following state boards: Alabama State Board of Social Work Examiners, Provider #0515; Florida Board of Clinical Social Work, Marriage and Family Therapy and Mental Health, Provider #50-2405; Illinois Division of Professional Regulation for Social Workers, License #159.001094; Illinois Division of Professional Regulation for Licensed Professional and Clinical Counselors, License #197.000185; Illinois Division of Professional Regulation for Marriage and Family Therapists, License #168.000190.

Special Approvals

This activity is designed to comply with the requirements of California Assembly Bill 1195, Cultural and Linguistic Competency.

About the Sponsor

The purpose of NetCE is to provide challenging curricula to assist healthcare professionals to raise their levels of expertise while fulfilling their continuing education requirements, thereby improving the quality of healthcare.

Our contributing faculty members have taken care to ensure that the information and recommendations are accurate and compatible with the standards generally accepted at the time of publication. The publisher disclaims any liability, loss or damage incurred as a consequence, directly or indirectly, of the use and application of any of the contents. Participants are cautioned about the potential risk of using limited knowledge when integrating new techniques into practice.

Disclosure Statement

It is the policy of NetCE not to accept commercial support. Furthermore, commercial interests are prohibited from distributing or providing access to this activity to learners.

Course Objective

The purpose of this course is to provide information that will allow health and mental health professionals to more easily comply with the Privacy and Security Rules defined by HIPAA.

Learning Objectives

Upon completion of this course, you should be able to:

1. Outline the history of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States.
2. Describe the Privacy Rule of HIPAA, including entities who must comply.
3. Identify protected health information and approaches to guarding and appropriately disclosing protected information.
4. Define patient rights and employers' responsibilities as delineated by HIPAA.
5. Evaluate the requirements of the HIPAA Security Rule.
6. Discuss sources of potential security breaches and approaches to avoidance and notifications.
7. Explain potential disciplinary actions for not complying with the HIPAA Privacy or Security Rule.

INTRODUCTION

To improve the efficiency and effectiveness of the healthcare system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required the U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of federal privacy protections for individually identifiable health information [1].

The HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule sets national standards for the protection of individually identifiable health information by three types of covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct standard healthcare transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (or April 14, 2004, for small health plans) [1].

The HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI). Compliance with the Security Rule was required as of April 20, 2005 (or April 20, 2006, for small health plans). The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules [1].

In 2013, the HHS enacted a final Omnibus rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health Act of 2009 (the HITECH Act) to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule [1].

All employees with access to PHI must receive HIPAA training soon after being hired. The Security Rule requires that each person who comes into contact with ePHI complete awareness training before gaining access to ePHI and that each person participate in refresher training at least annually. Companies are responsible for maintaining documentation of training completion for a period of six years. If significant changes are made to the HIPAA rules or a company's policy and procedures, all employees affected by the changes must receive updated training in a reasonable amount of time after the change becomes effective [2].

Please note that this activity is not intended to represent legal advice. For those interested in more detailed information, a list of resources that delve deeper is provided at the end of this course. In addition, all healthcare providers should review their company-specific policies and procedures relating to HIPAA.

HIPAA PRIVACY RULE

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) established, for the first time, a set of national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of individuals' health information (called protected health information or PHI) by organizations subject to the Privacy Rule (called covered entities) as well as standards for individuals' privacy rights to understand and control how their health information is used. Within the HHS, the Office for Civil Rights (OCR) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties [3].

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the healthcare marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed [3]. The Rule also gives individuals rights over their PHI, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their PHI in an electronic health record, and to request corrections [3].

WHO IS COVERED BY THE PRIVACY RULE?

Covered Entities

As noted, the Privacy Rule, as well as all the Administrative Simplification Rules, apply to health plans, healthcare clearinghouses, and to any healthcare provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA [3]. These groups are referred to collectively as covered entities.

Health Plans

Individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: those whose principal purpose is not providing or paying the cost of health care (e.g., the food stamps program), and those programs whose principal activity is directly providing health care (e.g., a community health center) or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, or property and casualty insurance. If an insurance entity has separable lines of business, one of which is a health plan, the HIPAA regulations apply to the entity with respect to the health plan line of business [3].

Healthcare Providers

Every healthcare provider, regardless of size, who electronically transmits health information in connection with certain transactions is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the HHS has established standards under the HIPAA Transactions Rule. Using electronic technology, such as e-mail, does not mean a healthcare provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a healthcare provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Healthcare providers include all providers of services (e.g., institutional providers such as hospitals) and providers of medical or health services (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care [3].

Healthcare Clearinghouses

Healthcare clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the healthcare clearinghouse's uses and disclosures of PHI. Healthcare clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions [3].

Hybrid Entities

A hybrid entity is a single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, nonhealth care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities [10]. Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a healthcare provider, or a healthcare clearinghouse. To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions (i.e., noncovered healthcare provider) or performs activities that would make the component a business associate of the entity if it were legally separate. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations [10].

For example, a university may be a single legal entity that includes an academic medical center's hospital that conducts electronic transactions for which the HHS has adopted standards. Because the hospital is part of the legal entity, the whole university, including the hospital, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the hospital as a health care component. The university also has the option of including in the designation other components that conduct covered functions or business associate-like functions. Most of the Privacy Rule's requirements would then only apply to the hospital portion of the university and any other designated components. The Privacy Rule would govern only the PHI created, received, or maintained by, or on behalf of, these components. PHI disclosures by the hospital to the rest of the university are regulated by the Privacy Rule in the same way as disclosures to entities outside the university [10].

Business Associates

The Privacy Rule also protects individually identifiable health information when it is created or maintained by a person or entity conducting certain functions on behalf of a covered entity, known as a business associate. A business associate is a person or entity who is not a member of the workforce and performs or assists in performing, for or on behalf of a covered entity, a function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule, involving the use or disclosure of individually identifiable health information, or that provides certain services to a covered entity that involve the use or disclosure of individually identifiable health information.

Because the HIPAA Administrative Simplification Rules do not directly regulate research activities, the Privacy Rule does not require a researcher or a research sponsor to become a business associate of a covered entity for research purposes. However, a covered entity may engage business associates to assist in de-identifying PHI, to prepare limited data sets, or to perform data aggregation. The Privacy Rule requires a covered entity to enter into a written contract, or another arrangement permitted by the Rule if both parties are government entities, with its business associates.

Generally, a covered entity may, for the purposes permitted by the Privacy Rule and specified in its written agreement with its business associate, disclose PHI to that business associate and allow the business associate to use, create, or receive PHI on its behalf. Before the covered entity discloses the PHI to the business associate, the covered entity must obtain satisfactory assurances, generally in the form of a contract, that the business associate will appropriately safeguard the information. With a few limited exceptions, the contract may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done directly by the covered entity [10].

PROTECTED HEALTH INFORMATION (PHI)

The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. As noted, the Privacy Rule calls this information protected health information or PHI [3].

Individually identifiable health information is defined as information, including demographic data, that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual and relates to the [3]:

- Individual's past, present, or future physical or mental health or condition
- Provision of health care to the individual
- Past, present, or future payment for the provision of health care to the individual

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

De-Identified Health Information

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information. A formal determination by a qualified statistician may be used to legally de-identify information. Alternatively, removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual [3].

MINIMUM NECESSARY CONCEPT

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity [11].

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use of, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to [11]:

- Disclosures to or requests by a healthcare provider for treatment purposes
- Disclosures to the individual who is the subject of the information
- Uses or disclosures made pursuant to an individual's authorization
- Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules
- Disclosures to the HHS when disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses or disclosures that are required by other law

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce [11].

Uses of, Disclosures of, and Requests for PHI

For uses of PHI, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit physicians, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification. For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the PHI disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required. For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of PHI necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly. Of course, where PHI is disclosed to, or requested by, healthcare providers for treatment purposes, the minimum necessary standard does not apply. In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request [3].

PHI DISCLOSURES

Permitted PHI Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose PHI without an individual's authorization for the following purposes or situations [3]:

- To the individual (unless required for access or accounting of disclosures)
- Treatment, payment, and healthcare operations
- Opportunity to agree or object
- Incident to an otherwise permitted use and disclosure
- Public interest and benefit activities
- Limited data set for the purposes of research, public health, or healthcare operations

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make [3].

Individual

A covered entity may disclose PHI to the individual who is the subject of the information.

Treatment, Payment, and Healthcare Operations

A covered entity may use and disclose PHI for its own treatment, payment, and healthcare operations activities. A covered entity also may disclose PHI for the treatment activities of any healthcare provider, the payment activities of another covered entity and of any healthcare provider, or the healthcare operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the PHI pertains to the relationship [3].

For the purposes of the Privacy Rule, treatment is defined as the provision, coordination, or management of health care and related services for an individual by one or more healthcare providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a healthcare provider to obtain payment or be reimbursed for the provision of health care to an individual [3].

Healthcare operations are any of the following activities [3]:

- Quality assessment and improvement activities, including case management and care coordination
- Competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation
- Conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs
- Specified insurance functions, such as underwriting, risk rating, and reinsuring risk
- Business planning, development, management, and administration
- Business management and general administrative activities of the entity, including but not limited to:
  - De-identifying PHI
  - Creating a limited data set
  - Certain fundraising for the benefit of the covered entity

Most uses and disclosures of psychotherapy notes for treatment, payment, and healthcare operations purposes require an authorization. Obtaining consent (written permission from individuals to use and disclose their PHI for treatment, payment, and healthcare operations) is optional under the Privacy Rule for all covered entities. The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent [3].

Uses and Disclosures with Opportunity to Agree or Object

Informal permission may be obtained by asking the individual outright or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual [3].

Facility Directories

It is a common practice in many healthcare facilities, such as hospitals, to maintain a directory of patient contact information. A covered healthcare provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.

The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation [3].

For Notification and Other Purposes

A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other designated persons any PHI directly relevant to that person's involvement in the individual's care or payment for care. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose PHI for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, PHI may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts [3].

Incidental Use and Disclosure

The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the minimum necessary [3].

Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for specific national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information [3].

Required by Law

Covered entities may use and disclose PHI without individual authorization as required by law (including by statute, regulation, or court orders).

Public Health Activities

Covered entities may disclose PHI to [3]:

- Public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect
- Entities subject to U.S. Food and Drug Administration (FDA) regulation regarding FDA-regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance
- Individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law
- Employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MHSA), or similar state law

Victims of Abuse, Neglect or Domestic Violence

In certain circumstances, covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

Health Oversight Activities

Covered entities may disclose PHI to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the healthcare system and government benefit programs.

Judicial and Administrative Proceedings

Covered entities may disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided [3].

Law Enforcement Purposes

Covered entities may disclose PHI to law enforcement officials for law enforcement purposes under the following circumstances, and subject to specified conditions [3]:

- As required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests
- To identify or locate a suspect, fugitive, material witness, or missing person
- In response to a law enforcement official's request for information about a victim or suspected victim of a crime
- To alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death
- When a covered entity believes that PHI is evidence of a crime that occurred on its premises
- By a covered healthcare provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime

Decedents

Covered entities may disclose PHI to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

Cadaveric Organ, Eye, or Tissue Donation

Covered entities may use or disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

Research

In the context of HIPAA, research is considered any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose PHI for research purposes, without an individual's authorization, provided the covered entity obtains either [3]:

- Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of PHI about them for research purposes has been approved by an Institutional Review Board or Privacy Board.
- Representations from the researcher that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any PHI from the covered entity, and that PHI for which access is sought is necessary for the research.
- Representations from the researcher that the use or disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.

A covered entity also may use or disclose, without an individuals' authorization, a limited data set of PHI for research purposes.

Serious Threat to Health or Safety

Covered entities may disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal [3].

Essential Government Functions

An authorization is not required to use or disclose PHI for certain essential government functions. Such functions include [3]:

- Assuring proper execution of a military mission or conducting intelligence and national security activities that are authorized by law
- Providing protective services to the President
- Making medical suitability determinations for U.S. State Department employees
- Protecting the health and safety of inmates or employees in a correctional institution
- Determining eligibility for or conducting enrollment in certain government benefit programs

Workers' Compensation

Covered entities may disclose PHI as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses [3].

Limited Data Set

A limited data set defined as is PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, healthcare operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the PHI within the limited data set [3].

Authorizations for PHI Release

A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or healthcare operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances [3]. Covered entities must establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures or requests for disclosures that limits the PHI disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

An authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes [3].

All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data [3].

A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with a few exceptions [3]. Covered entities who originate the notes may use them for treatment. In addition, a covered entity may use or disclose, without an individual's authorization, psychotherapy notes:

- For its own training
- To defend itself in legal proceedings brought by the individual
- For the HHS to investigate or determine the covered entity's compliance with the Privacy Rules
- To avert a serious and imminent threat to public health or safety
- To a health oversight agency for lawful oversight of the originator of the psychotherapy notes
- For the lawful activities of a coroner or medical examiner
- As required by law

PHI Release During Emergencies

During a severe disaster, including infectious disease outbreak or natural disaster, providers and health plans covered by the HIPAA Privacy Rule can share patient information in specifically delineated ways. For example, healthcare providers can share patient information as necessary to provide treatment, including [4]:

- Sharing information with other providers (including hospitals and clinics)
- Referring patients for treatment (including linking patients with available providers in areas where the patients have relocated)
- Coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services)

Providers can also share patient information to the extent necessary to seek payment for these healthcare services.

Healthcare providers are permitted to share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death. The healthcare provider should get verbal permission from individuals, when possible; however, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgement, doing so is in the patient's best interest [4].

Providers are able to share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public, consistent with applicable law and the provider's standards of ethical conduct.

NOTICE OF PRIVACY PRACTICES

Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose PHI and must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice should describe individuals' rights, including the right to complain to the HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other healthcare providers, and health plans [3].

Notice Distribution

A covered healthcare provider with a direct treatment relationship with individuals must have delivered a privacy practices notice to patients [3]:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery)

- By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice
- In emergency treatment situations, as soon as practicable after the emergency abates

Covered entities, whether direct treatment providers or indirect treatment providers (such as laboratories) or health plans must supply notice to anyone on request. A covered entity must also make its notice electronically available on any website it maintains for customer service or benefits information [3].

The covered entities in an organized healthcare arrangement may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the PHI created or received in connection with participation in the arrangement. Distribution of a joint notice by any covered entity participating in the organized healthcare arrangement at the first point that an organized healthcare arrangement member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized healthcare arrangement [3].

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

Acknowledgement of Notice Receipt

A covered healthcare provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice. The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation [3].

PATIENT RIGHTS

Access

Except in certain circumstances, individuals have the right to review and obtain a copy of their PHI in a covered entity's designated record set. The designated record set is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. The Rule excepts from the right of access the following PHI:

- Psychotherapy notes
- Information compiled for legal proceedings
- Laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access
- Information held by certain research laboratories

For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a healthcare professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed healthcare professional for a second opinion. Covered entities may impose reasonable, cost-based fees for the cost of copying and postage [3].

Amendment

The Rule gives individuals the right to have covered entities amend their PHI in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend PHI in its designated record set upon receipt of notice to amend from another covered entity [3].

Disclosure Accounting

Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures [3]:

- For treatment, payment, or healthcare operations
- To the individual or the individual's personal representative
- For notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories
- Pursuant to an authorization
- Of a limited data set
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody
- Incident to otherwise permitted or required uses or disclosures

Accounting for disclosures to health-oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

Restriction Request

Individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment, or healthcare operations; disclosure to persons involved in the individual's health care or payment for health care; or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency [3].

Confidential Communications Requirements

Health plans and covered healthcare providers must permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the covered entity typically employs. For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a postcard.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the PHI could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled [3].

Personal Representatives

The Privacy Rule requires a covered entity to treat a personal representative the same as the individual, with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under the Rule. A personal representative is a person legally authorized to make healthcare decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual or that treating the person as the personal representative could otherwise endanger the individual [3].

Minors

In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to state and other law to determine the rights of parents to access and control the PHI of their minor children. If state and other law is silent concerning parental access to the minor's PHI, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed healthcare professional in the exercise of professional judgment [3].

EMPLOYERS' RESPONSIBILITIES

Privacy Official and HIPAA Policies and Procedures

The HHS recognizes that covered entities range from the smallest provider to the largest, multistate health plan. Therefore, the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources [3].

With this in mind, all covered entities must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. A covered entity must also designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices [3].

Workforce Training and Management

A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. Workforce members include employees, volunteers, trainees, and other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity). A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule [3].

Mitigation

A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule [3].

Data Safeguards

A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing PHI before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes [3].

Complaints

A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice. Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS [3].

Retaliation and Waiver

A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by the HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility [3].

Documentation and Record Retention

A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

Fully Insured Group Health Plan Exception

The only administrative obligations with which a fully insured group health plan that has no more than enrollment data and summary health information is required to comply are the ban on retaliatory acts and waiver of individual rights and documentation requirements with respect to plan documents, if such documents are amended to provide for the disclosure of PHI to the plan sponsor by a health insurance issuer or HMO that services the group health plan.

Marketing and Sale of PHI

Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. The Privacy Rule carves out the following health-related activities from this definition of marketing [3]:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan
- Communications for treatment of the individual
- Communications for case management or care coordination for the individual or to direct or recommend alternative treatments, therapies, healthcare providers, or care settings to the individual

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses PHI in exchange for direct or indirect remuneration for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose PHI for marketing, except for face-to-face marketing communications between a covered entity and an individual and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition [3].

HIPAA SECURITY RULE

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the healthcare industry. At the same time, new technologies were evolving, and the healthcare industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information, and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHRs), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient, the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the healthcare marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI [5].

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities, or assessments. A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI [5].

SECURITY RULE REQUIREMENTS

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must [5]:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

The Security Rule defines confidentiality to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, integrity means that e-PHI is not altered or destroyed in an unauthorized manner, while availability means that e-PHI is accessible and usable on demand by an authorized person [5].

When a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider [5]:

- Its size, complexity, and capabilities
- Its technical, hardware, and software infrastructure
- The costs of security measures
- The likelihood and possible impact of potential risks to e-PHI

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

Covered entities are required to comply with every Security Rule standard. However, the Security Rule categorizes certain implementation specifications within those standards as addressable, while others are required. The required implementation specifications must be implemented. The addressable designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate [5].

Risk Analysis and Management

The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately because, by helping to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule [5].

A risk analysis process includes, but is not limited to, the following [5]:

- Evaluating the likelihood and impact of potential risks to e-PHI
- Implementing appropriate security measures to address the risks identified in the risk analysis
- Documenting the chosen security measures and, where required, the rationale for adopting those measures
- Maintaining continuous, reasonable, and appropriate security protections

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI [5].

Physical Safeguards

Facility Access and Control

A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed [5].

Workstation and Device Security

A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media to ensure appropriate protection of e-PHI [5].

Technical Safeguards

Access Control

A covered entity must implement technical policies and procedures that allow only authorized persons to access e-PHI [5].

Audit Controls

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI [5].

Integrity Controls

A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed [5].

Transmission Security

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network [5].

Administrative Safeguards

Security Management Process

As explained, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level [5].

Security Personnel

A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures [5].

Information Access Management

Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the minimum necessary, the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (i.e., role-based access) [5].

Workforce Training and Management

A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures [5].

Evaluation

A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule [5].

BREACHES

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors [6]:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

Covered entities and business associates have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the PHI has been compromised [6].

There are three exceptions to the definition of breach. The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized healthcare arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information [6].

Notification Rules

Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

A covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate, and, if it discovers additional information, submit updates. If only one option is available in a particular submission category, the covered entity should pick the best option and may provide additional details in the free text portion of the submission [6].

Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or by other means [6].

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, and a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate) [6].

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual [6].

If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report [7].

Breaches Affecting 500 or More Individuals

If a breach of unsecured PHI affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by visiting https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf [7].

Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured PHI affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. A covered entity is not required to wait until the end of the calendar year to report and may report sooner at their discretion. The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity should submit the notice electronically by visiting https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf [7].

Administrative Responsibilities and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required. If notification was not required, documentation may include the entity's risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure or the application of any other exceptions to the definition of breach [6].

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures [6].

HIPAA ENFORCEMENT

The OCR is responsible for enforcing the Privacy and Security Rules. It does so through an established complaint resolution process. The OCR enforces the Privacy and Security Rules by [8]:

- Investigating filed complaints
- Conducting compliance reviews to determine if covered entities are in compliance
- Performing education and outreach to foster compliance with the Rules' requirements

The OCR also works in conjunction with the Department of Justice to refer possible criminal violations of HIPAA.

MANDATED AUDITS

The HITECH Act requires the HHS to periodically audit covered entities and business associates for their compliance with the HIPAA Rules. The audit program is an important part of the OCR's overall health information privacy, security, and breach notification compliance activities. The OCR uses the audit program to assess the HIPAA compliance efforts of a range of entities covered by HIPAA regulations. The audits present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable OCR to get out in front of problems before they result in breaches. In 2016–2017, the OCR conducted audits of 166 covered entities and 41 business associates [9]. Each covered entity and business associate is eligible for an audit.

DISCIPLINARY ACTIONS

The OCR is responsible for administering and enforcing HIPAA standards and may conduct complaint investigations and compliance reviews. Consistent with the principles for achieving compliance, the OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations may be subject to criminal prosecution.

Civil Money Penalties

The OCR may impose a penalty on a covered entity for a failure to comply with a requirement. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement [3].

A penalty will not be imposed for violations in certain circumstances, such as if [3]:

- The failure to comply was not due to willful neglect and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of the OCR).
- The Department of Justice has imposed a criminal penalty for the failure to comply.

In addition, the OCR may choose to reduce a penalty if the failure to comply was due to reasonable cause and the penalty would be excessive given the nature and extent of the noncompliance.

Before the OCR imposes a penalty, it will notify the covered entity and provide the covered entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be submitted to the OCR within 30 days of receipt of the notice. In addition, if the OCR states that it intends to impose a penalty, a covered entity has the right to request an administrative hearing to appeal the proposed penalty [3].

Criminal Penalties

A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy or Security Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm. Again, the Department of Justice is responsible for criminal prosecutions [3].

STATE LAWS

In general, state laws that are contrary to the Privacy or Security Rule are preempted by the federal requirements, which means that the federal requirements will apply. The Privacy and Security Rules provide exceptions to the general rule of federal preemption for contrary state laws that [3]:

- Relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information
- Provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention
- Require certain health plan reporting, such as for management or financial audits

In addition, preemption of a contrary state law will not occur if the HHS determines, in response to a request from a state or other entity or person, that the state law [3]:

- Is necessary to prevent fraud and abuse related to the provision of or payment for health care
- Is necessary to ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation
- Is necessary for state reporting on health care delivery or costs
- Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy or Security Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served
- Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances, or that is deemed a controlled substance by state law

CONCLUSION

The HIPAA Rules are flexible and scalable to accommodate the enormous range in types and sizes of entities that must comply with them. While this course has provided an overview of the legal standards and requirements of the HIPAA Privacy and Security Rules, it is vital that healthcare professionals remain current on their facility's and state's rules and regulations related to the protection of PHI.

RESOURCES

HealthIT.gov
Privacy and Security Resources for Providers
https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

U.S. Department of Health and Human Services
HIPAA for Professionals
https://www.hhs.gov/hipaa/for-professionals

American Medical Association
https://www.ama-assn.org/practice-management/hipaa/hipaa-privacy-rule

U.S. Department of Health and Human Services Office for Civil Rights
https://www.hhs.gov/ocr

Works Cited

1. U.S. Department of Health and Human Services. HIPAA for Professionals. Available at https://www.hhs.gov/hipaa/for-professionals/index.html. Last accessed September 23, 2022.
2. Harp F. *HIPAA Privacy 2022*. Denver, CO: TRC Healthcare; 2022.
3. U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. Available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Last accessed September 23, 2022.
4. U.S. Department of Health and Human Services. FAQs: Can Health Care Information Be Shared in a Severe Disaster? Available at https://www.hhs.gov/hipaa/for-professionals/faq/960/can-health-care-information-be-shared-in-a-severe-disaster/index.html. Last accessed September 23, 2022.
5. U.S. Department of Health and Human Services. Summary of the HIPAA Security Rule. Available at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Last accessed September 23, 2022.
6. U.S. Department of Health and Human Services. Breach Notification Rule. Available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Last accessed September 23, 2022.
7. U.S. Department of Health and Human Services. Submitting Notice of a Breach to the Secretary. Available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html. Last accessed September 23, 2022.
8. U.S. Department of Health and Human Services. Enforcement Process. Available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html. Last accessed September 23, 2022.
9. U.S. Department of Health and Human Services. HIPAA Privacy, Security, and Breach Notification Audit Program. Available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html. Last accessed September 23, 2022.
10. National Institutes of Health. To Whom Does the Privacy Rule Apply and Whom Will It Affect? Available at https://privacyruleandresearch.nih.gov/pr_06.asp. Last accessed September 23, 2022.
11. U.S. Department of Health and Human Services. Minimum Necessary Requirement. Available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html. Last accessed September 23, 2022.