Mindful
Continuing Education

Summarizing the HIPAA Privacy Rule

Introduction

The Health Insurance Portability and Accountability Act Privacy Rule provides patients with essential privacy rights and protections concerning their health information. Providers must understand when it is appropriate to share the protected health information of an individual being treated for a behavioral health condition. All healthcare providers are responsible for understanding what information is protected and implementing HIPAA requirements regarding how the protected health information can be used and disclosed.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was implemented in 1996 by the Department of Health and Human Services. HIPAA is a federal law establishing national standards to protect patients' health information from being disclosed without their knowledge or consent. The HIPAA Privacy Rule was established in December 2000 and modified in August 2002 to implement the requirements of HIPAA. While HIPAA's Privacy Rule safeguards protected health information, the Security Rule was established in 2003 and creates national standards for electronically protected health information (OCR, 2022 & CDC, 2022).

What is The Privacy Rule?

The Privacy Rule sets national standards for protecting individually identifiable health information. In addition, it establishes the use and disclosure of protected health information (PHI) by covered entities. It also creates standards for individuals to help them understand their health information and control its use. The Privacy Rule applies to three types of covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct any healthcare transactions electronically. All entities have been required to comply with the Privacy Rule since April 14, 2004.

The Rule requires safeguards to be in place to protect the privacy of protected health information and set limitations on the uses and disclosures that can be made without an individual's consent. The Rule gives individuals rights over their PHI, including the right to examine and make copies of their health record, the right to direct an entity to share electronic copies of their protected health information to a third party via an electronic health record, and the right to request corrections.

The Privacy Rule aims to protect an individual's health information while providing access to health information needed for an individual's health care and for protecting the general population's health and well-being. Within the Department of Health and Human Services, the Office for Civil Rights is responsible for implementing and enforcing the Privacy Rule, including an entity's compliance, as well as assessing fines for failure to follow the Privacy Rule (OCR, 2022).

Covered Entities

HIPAA rules apply to individual health providers and organizations who conduct any health care transactions electronically; they are called HIPAA-covered entities. There are three types of entities are as follows:

Health Plans

Health plans include health insurance companies, health maintenance organizations (HMOs), employer-sponsored health plans, church-sponsored health plans, and government programs that pay for health care (Medicare, Medicaid, military health programs, and veteran health plans). Health plans can include health, dental, vision, and prescription drug insurers and long-term care insurers. Exceptions are discussed below.

- Group health plans administered by an employer with less than 50 participants are not covered entities.
- The following government-funded programs are not considered covered entity health plans:
    - Programs that do not provide or pay for health care, such as food stamps
    - Programs that provide direct health care, such as community health centers or programs that provide grant funding for health care.
- Insurance entities that are not considered covered entities include:
    - Insurance programs that only provide workman's compensation
    - Vehicle Insurance
    - Property Insurance

- Casualty Insurance

If an insurance company has multiple business areas, their health insurance programs would be subject to HIPAA Privacy Rules while their other areas of business would not (OCR, 2022).

Health Care Clearinghouses

Clearinghouses are organizations that process non-standard health information to comply with standards for data content or vice versa on behalf of another organization. Examples of healthcare clearinghouses include:

- Billing services
- Repricing companies
- Community health management information systems
- Value-added networks if they perform clearinghouse functions (OCR, 2022)

Health Care Providers

All healthcare providers, regardless of size, who submit transactions of health information electronically, are covered entities and must comply with HIPAA Privacy Rules. These transactions can include benefits eligibility inquiries, claim status, payment and remittance advice, coordination of benefits, claims and encounter information, enrollment and disenrollment, referral authorization requests, premium payment, and any other transaction in which there are standards under the HIPAA Transaction Rule. The Privacy Rule covers health care providers whether they directly electronically submit the transitions, use a billing service, or use a third party to transmit on their behalf. Health care providers include institutional providers such as hospitals or nursing homes and individual providers such as doctors, dentists, chiropractors, pharmacies, psychologists, behavioral health providers, and any other individual or organization that provides, bills, or is paid for health care. (OCR, 2022 & CMS, 2022).

Business Associates

The HIPAA Privacy Rule only applies to covered entities, but many entities contract with other individuals or businesses to help run their day-to-day operations. The Privacy Rule

allows covered entities to disclose protected health information with business associates if they have satisfactory assurances from the business associate in writing, either as a contract or other written agreement, that the business associate will safeguard the PHI it receives from, or creates for, the covered entity. The business associates agree that they will only use the protected health information they receive or create for the services they were hired to provide and that they will protect the information from misuse. They will also comply with the entity's expectations under the Privacy Rule. Covered entities can disclose protected health information to the business associate only to provide the covered entities' health care functions. The business associates are to only use the information for their independent business purposes beyond what is needed for their management and administration requirements (OCR, 2019).

A business associate is an individual or organization that performs services that involve protected health information on behalf of a covered entity. An employee of the covered entity is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse could be a business associate of another covered entity. Services a business associate might provide include:

- Claims processing or administration
- Data analysis, processing, or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Practice management
- Repricing (OCR, 2019)

Business associate services and examples include:

- **Legal:** A lawyer whose legal services allow access to protected health information.
- **Actuarial:** An actuarial service analyzing the rates of disability and life span.
- **Accounting:** A CPA whose accounting services to a healthcare provider involve access to protected health information.

- **Consulting:** A consultant who performs utilization reviews for a hospital.
- **Data aggregation:** A healthcare clearinghouse that modifies a claim from a non-standard transaction into a standard format on behalf of a healthcare provider and forwards the processed transaction to a payer.
- **Management:** A pharmacy benefits manager who manages a health plan's pharmacist network.
- **Administrative:** An independent medical transcriptionist that provides transcription services to a physician.
- **Accreditation:** An accreditation organization reviewing a program's compliance.
- **Financial:** A third-party administrator who assists a health plan with claims processing (OCR, 2019).

Business Associate Contract

A covered entity that uses a business associate to assist in the daily operations of its healthcare activities and functions is required to have a written business associate contract that clearly states what specific activities the business associate does for the covered entity and that the business associate complies with HIPAA.

Business associates' written contracts must include the following:

- A description of the permitted uses and required uses of protected health information
- A provision that they will not use or disclose the protected health information beyond what is permitted by the contract or required by law
- A requirement is that they use appropriate safeguards to prevent the use or disclosure of protected health information outside of the contracted use (CMS, 2022 & OCR, 2022).

Should a covered entity become aware of an information breach or violation by a business associate, the covered entity must take steps to rectify or end the violation. If steps are unsuccessful, the covered entity must terminate the contract. If contract termination is not possible, the entity must report the problem to the Department of Health and Human Services Office for Civil Rights (OCR, 2019).

Exceptions to the Business Associate Requirement

The Privacy Rule allows for the following exceptions where the covered entity does not need to have a business associate contract before the protected health information can be disclosed:

- A covered entity's disclosure to a health care provider for treatment of the individual. Examples include:
    - A hospital sharing a medical chart for treatment purposes with a specialist the hospital has referred a patient to
    - A physician sharing protected health information with a laboratory for the treatment of a patient
    - A hospital laboratory disclosing protected health information to a reference laboratory for the patient's treatment.
- A group health plan, a health insurance issuer, or HMO that provides health insurance benefits or coverage for a group health plan disclosing information to the health plan sponsor. The group health plan's documents must have been amended to limit the information disclosed.
- A public benefits health plan program collects and shares PHI with an agency other than the agency administering the health plan that collects PHI to determine eligibility for the government program and subsequent enrollment.
- A healthcare provider disclosing PHI to a health plan for payment purposes or when the healthcare provider accepts a discounted rate to participate in the health plan's network. A provider who submits a claim to a health plan and a health plan that pays the claim are acting on their own accord as a covered entity.
- A person or organization whose functions or services do not require access to PHI and where any access to PHI by such persons would be incidental (ex., a janitor or electrician).
- A person or organization that acts as a conduit for PHI (ex. the US Postal Service, private couriers).
- Covered entities who participate in an organized healthcare arrangement (OHCA) make disclosures related to the joint healthcare activities of the OHCA.

- A group health plan purchases insurance from a health insurance issuer. The Privacy Rule defines the relationship between the group health plan and the health insurance issuer as an organized healthcare arrangement concerning the individuals they jointly serve. These covered entities are allowed to share protected health information related to the joint healthcare activities of the OHCA.
- A covered entity purchases a health plan product or insurance; each entity acts on its own accord when the covered entity purchases the insurance benefits and when the covered entity submits a claim and the insurer pays the claim.
- Disclosing PHI for research purposes, either with patient authorization or as a limited data set.
- A financial institution processing consumer-conducted financial transactions by debit, credit, or other payment cards or checks, processes electronic funds transfers, or conducts other activities that directly facilitate the transfer of funds for payment for health care or health insurance premiums. When it provides these services, the financial institution provides standard banking or financial transaction services to its customers. It is not performing a function or activity for or on behalf of the covered entity (OCR, 2019).

Case Example

A complaint alleged that a law firm working on behalf of a pharmacy in an administrative proceeding impermissibly disclosed the protected health information of a pharmacy's customer. OCR found no evidence that the law firm had impermissibly disclosed the customer's PHI during its investigation of the allegation. However, OCR's investigation did reveal that the pharmacy and the law firm had not entered into a business associate agreement to ensure that PHI is appropriately safeguarded and as required by the Privacy Rule. Without a proper business associate contract, the pharmacy may not disclose PHI to the law firm. Therefore, OCR required the pharmacy chain and the law firm to enter into a business associate agreement, thus resolving the matter (OCR, 2017)

Protected Health Information

Protected health information (PHI) under the Privacy Rule covers all individually identifiable health information held or transmitted by a covered entity or business associate in any form or media, including electronic, paper, or oral.

Individually identifiable health information includes demographic data that identifies or can reasonably be expected to identify the individual. It includes:

- The individual's past, present, and future physical or mental health condition
- The individual's provision of health care
- The individual's past, present, and future payment for the provision of health care
- Any data that identifies the individual or provides sufficient information so that the individual could reasonably be identified (this information could include name, address, birth date, or social security number) (OCR, 2022).

Employment records maintained by a covered entity that may contain health or education information are not considered protected health information and are not covered by the Privacy Rule.

De-identified health information is not considered protected health information and has no restrictions on its use or disclosure. For information to be considered de-identified health information, there needs to be no basis that an individual could be identified. The two approved ways for health information to be de-identified are:

- A formal determination by a qualified statistician
- Removal of an individual's specific identifiers, including relatives, household members, and employers, is only deemed adequate if the covered entity does not know that the remaining data could be used to identify the person (OCR, 2022).

Uses & Disclosures of Protected Health Information

One of the primary goals of the Privacy Rule is to establish and limit the situations where an individual's protected health information can be used and disclosed by a covered entity. Accordingly, a covered entity can only use or disclose protected health information as allowed or required by the Privacy Rule or as the individual (or a designated representative) authorizes in writing.

Required Disclosures

A covered entity must disclose protected health information to individuals (or their representatives) when they request access to their PHI or a list of disclosures of their PHI.

Entity representatives must also disclose PHI to the Department of Health and Human Services if they complete a compliance review, investigate a complaint, or enforce action (OCR, 2022).

Permitted Uses & Disclosures

The Office of Civil Rights (2022) identifies the following areas a covered entity is allowed, but not required, to use and disclose protected health information without the individual's authorization.

To the Individual

A covered entity can disclose PHI to the person who is the subject of the PHI.

Treatment, Payment, and Health Care Operations

A covered entity can use and disclose PHI for its own treatment, payment, and healthcare activities. A covered entity can disclose PHI for any healthcare provider’s treatment activities, the payment activities of any healthcare provider or another covered entity, or the healthcare operations involving either competency, quality assurance activities, fraud and abuse detection, and compliance activities of another covered entity, if both entities have a relationship with the individual, or have in the past, and the PHI pertains to the relationship.

Most psychotherapy notes use and disclosures for treatment, payment, and health care operations purposes require authorization. Written consent from the individual is optional under the Privacy Rule for the use and disclosure of the individual's PHI for treatment, payment, and health care operations for all covered entities. The process of obtaining consent and the content of the consent form can be determined by the covered entity choosing to acquire consent.

Treatment

Treatment by one or more healthcare providers includes providing, coordinating, and managing an individual's healthcare and related services. This includes consultation between providers and referrals of a patient to another provider.

Payment

Payment activities of a health plan include obtaining premiums, determining or fulfilling responsibilities for coverage, providing benefits, and furnishing or obtaining reimbursement for health care delivered to an individual. Payment activities of a healthcare provider include obtaining payment or reimbursement for the provision of health care to an individual.

Health Care Operations

These include any of the following activities:

- Quality review and improvement activities, which may include care coordination and case management
- Competency assurance activities, which may include performance evaluations, credentialing, and accreditation of providers or health plans
- Arranging for or conducting medical reviews, audits, or legal services, which may include fraud and abuse detection and compliance programs
- Specified insurance functions, which may include underwriting, risk rating, and reinsuring risk
- Business development, planning, management, and administration
- General administrative activities of the entity, which may include de-identifying protected health information, creating limited data sets, or fundraising for the benefit of the covered entity (OCR, 2022).

Opportunity to Agree or Object

Informal permission may be acquired by asking the individual verbally or by other circumstances that give the individual the option to agree or object. In situations where the individual is incapable (emergency situation) or unavailable, a covered entity's representatives may be allowed to use and disclose the information if, in their professional judgment, the use or disclosure of the information is determined to be in the best interest of the individual.

Facility Directories

Many healthcare facilities (hospitals, nursing homes) have a directory of patient contact information. A covered entity is allowed to rely on an individual's informal permission to be

listed in its facility directory with information including the patient's name, condition, religious affiliation, and location in the facility. The provider is allowed to disclose the individual's location in the facility and condition to anyone asking for the person by name. Providers may also disclose to the clergy the person's religious affiliation. Clergy members are not required to ask for the person by name when inquiring about a patient's religious affiliation.

For Notification and Other Purposes

A covered entity is allowed to use a patient's informal permission to share information with the patient's family, relatives, or friends or with any other person who the patient identifies, PHI that is directly related to the person's involvement in the patient's care or payment for care. An example of this provision is when a pharmacist releases a filled prescription to a person acting on behalf of a patient. A covered entity may use an individual's informal permission to use or disclose PHI to identify, locate, and notify family members, representatives, or another person responsible for the individual's care, of the individual's location, general condition, or death. Protected health information can be disclosed to public or private entities authorized by law for notification purposes to assist in disaster relief efforts (OCR, 2022).

Incidental Use or Disclosure

The Privacy Rule does not require or expect that every risk of use or disclosure of protected health information will be eliminated. Use or disclosure of PHI that occurs as a result of, or as an incident to, an otherwise allowed use or disclosure is permitted as long as the covered entity has implemented reasonable safeguards and the information being shared follows the minimum necessary guidelines, as required by the Privacy Rule (OCR, 2022).

Public Interest and Benefit Activities

The Privacy Rule allows for the use and disclosure of protected health information for twelve national priority purposes without an individual's authorization or permission. The Privacy Rule recognizes the importance of health information outside of the healthcare context, and therefore the following disclosures are allowed but not required. Specific conditions and limitations apply to each public interest purpose, seeking a balance between an individual's privacy interest and the public interest need for the information.

1. **Required by Law**

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

2. **Public Health Activities**

   Covered entities can disclose protected health information to:

   - Public health authorities collecting and receiving information for the prevention or control of disease, injury, or disability as authorized by law and to public health or government authorities authorized to receive reports of child abuse and neglect.
   - Entities subject to FDA regulation regarding FDA-regulated products or services for adverse event reporting, tracking of products, recalls of products, and surveillance post-marketing
   - Persons who may have been exposed to or contracted a communicable disease if the law authorizes notification
   - When requested by employers, regarding employees, for information surrounding a work-related illness, injury, or workplace-related medical surveillance, should such information be required by the employer to adhere to the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.

3. **Victims of Abuse, Neglect, or Domestic Violence**

   Covered entities can disclose PHI to necessary legal or government authorities regarding victims of abuse, neglect, or domestic violence, under certain circumstances.

4. **Health Oversight Activities**

   Covered entities can disclose PHI to health oversight agencies so they can complete legally authorized health oversight activities. These may include audits and investigations to oversee government benefit programs or the healthcare system.

5. **Judicial and Administrative Proceedings**

   Covered entities can share PHI in a judicial or administrative proceeding if the requested information is through a court order or administrative tribunal. Protected health information can be released in response to a subpoena or other lawful

process if safeguards are implemented regarding notice to the individual or a protective order is provided.

6. **Law Enforcement Purposes**

   Covered entities can disclose PHI under specific conditions to law enforcement personnel under the following six circumstances:

   - As required by law or administrative requests (court orders, court-ordered warrants, subpoenas)
   - To identify or locate a material witness, fugitive, suspect, or missing person.
   - In response to a law enforcement request for information regarding a victim or suspected crime victim
   - To alert law enforcement of an individual's death should the covered entity suspect that criminal activity may have caused the death.
   - If a covered entity suspects that PHI is evidence of a crime that occurred at the covered entity's location.
   - If a healthcare provider was involved in a medical emergency not occurring at the covered entity's location to inform law enforcement of the commission of a crime, the location of the crime, the identification of crime victims, and the identification of the perpetrator of the crime.

7. **Decedents**

   Protected health information can be disclosed from covered entities to funeral directors and to medical examiners or coroners to aid in identifying a deceased person, determining the cause of death, and performing other functions authorized by law.

8. **Cadaveric Organ, Eye, or Tissue Donation**

   Covered entities can use or disclose PHI to assist in the donation and transplantation of cadaveric organs, eyes, and tissue.

9. **Research**

The Privacy Rule allows a covered entity to use and disclose PHI without an individual's authorization for research purposes under any of the following circumstances:

- An Institutional Review Board or Privacy Board has approved a waiver of the individual's authorization for the use or disclosure of their PHI about them for research purposes.
- The researcher's use or disclosure of PHI is only to prepare a research protocol or similar preparatory steps toward research. Access to the PHI is necessary for the research. No protected health information will be removed from the covered entity by the researcher.
- The researcher's use and disclosure are for the purpose of research on the PHI of descendants, and the PHI is necessary for the research. The covered entity may request documentation of the individual's death on whom the information is being requested.

A covered entity may also use or disclose a limited data set of protected health information for research purposes without an individual's authorization.

10. **Serious Threat to Health or Safety**

Covered entities can share PHI they believe is necessary to prevent or limit a serious and imminent threat to a person or the public. However, the disclosure must be made to someone the covered entity believes can prevent or limit the threat or target of the threat. For example, they can disclose necessary information to law enforcement to identify or apprehend an escapee or violent criminal.

11. **Essential Government Functions**

Certain essential government functions do not require authorization to use or disclose protected health information. These functions include:

- Assuring a military mission is properly executed
- Conducting legally authorized intelligence and national security activities
- Providing Presidential protective services
- Making U.S. State Department employee's medical suitability determinations

- Protecting the health and safety of correctional institution inmates or employees
- Determining government benefit program eligibility or conducting enrollment in programs

12. **Workers' Compensation**

    Workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses are authorized to access protected health information, and covered entities may disclose information to comply with those laws.

Limited Data Set

A limited data set is PHI, where specific individual identifiers for the individual, their relatives, household members, and employers have been removed. Limited data set information can be used for research, public health purposes, or health care operations. The recipient of the information must have a data use agreement ensuring safeguards for the PHI within the data set (OCR, 2022).

Authorized Uses & Disclosures

A covered entity must obtain an individual's written consent for any use or disclosure of protected health information that does not fall under the categories of treatment, payment, health care operations, or information that is permitted or required by the Privacy Rule. Except in limited circumstances, a covered entity can not make a condition of enrollment, treatment, payment, or benefits eligibility on an individual granting authorization.

Authorization

An authorization must be written in specific terms. The authorization can allow for the use and disclosure of PHI by the covered entity seeking authorization or by a third party. Authorizations should be written in simple and direct language, specify the information to be used or disclosed, identify the person(s) receiving and disclosing the information, authorization expiration, the individual's right to revoke in writing, and other data.

Examples of an individual's disclosure authorization include:

- disclosures to a life insurer for coverage purposes
- disclosures to an employer for pre-employment lab tests or physical results
- disclosures to a pharmaceutical organization for marketing purposes (OCR, 2022).=

Psychotherapy Notes

A covered entity must obtain an individual's consent to use or disclose psychotherapy notes. However, the covered entity who created the notes can use them for treatment. The covered entity can use or disclose, without an individual's authorization, the psychotherapy notes for:

- Its own training
- To defend itself in legal proceedings brought against them by the individual
- For an HHS investigation or determination of the covered entity's compliance with the Privacy Rules
- To prevent a serious and imminent threat to public safety or health
- For a health oversight agency for legal oversight of the psychotherapy notes origination
- A coroner or medical examiner's lawful activities
- Purposes required by law (OCR, 2022)

Marketing

Marketing is any type of communication about a product or service that encourages the recipient to use or purchase the product or service. The covered entity must first obtain the individual's consent if the communication is considered marketing. Marketing also includes arrangements between a covered entity and another organization where the covered entity would disclose PHI to the organization in exchange for direct or indirect compensation for the organization to communicate about its products or services to encourage the recipient to purchase and use the service or product. The individual must consent to the marketing before it happens, and if the covered entity is receiving compensation, it must be identified on the individual's authorization. A covered entity cannot sell PHI to another organization for its own purposes.

The Privacy Rule does not consider the following health-related communications to be marketing:

- Descriptions or payments of health-related products or services included in or provided by a benefit plan of the covered entity making the communication.
- Information about participating providers in a health plan network, enhancements or replacements to a health plan, and added-value health-related products or services available exclusively to a health plan's enrollees that are not part of the benefits plan.
- Individual treatment communications.
- Case management or care coordination communications for the individual. These include directions or recommendations of therapies, alternative treatments, care settings, or communication with the individual's health care providers (OCR, 2022).

Limiting Uses and Disclosures

Minimum Necessary

Covered entities must limit unnecessary or inappropriate disclosure of protected health information and should only request the minimum necessary PHI needed to provide treatment. They should make reasonable efforts to only use, disclose, or request the minimum necessary PHI to accomplish their treatment needs. Covered entities must develop and implement policies and procedures that support minimum and necessary disclosure. A covered entity may not request an entire medical record unless it can specifically justify the need for the complete record.

Exceptions to the minimum necessary principle are:

- A healthcare provider for treatment
- An individual who is the subject of the PHI or a designated personal representative
- Authorization for the use or disclosure
- HHS for a compliance review, complaint investigation, or enforcement
- Required by law

- Required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules (OCR, 2022).

Access & Uses

A covered entity's representatives must develop and implement internal uses policies and procedures for members of their workforce, their roles, and who has access and uses to protected health information based on their role needs. The policies and procedures must identify the people, or groups of people who require access to protected health information to complete their job duties, the categories of protected health information they need access to, and any conditions under which they need the information to do their jobs (OCR, 2022).

Disclosures and Requests for Disclosures

Policies and procedures or standard protocols must be established and implemented by covered entities for routine, recurring disclosures or requests for disclosures. The PHI to be released must be limited to that which is the minimum necessary for meeting the need of the disclosure and for eliminating the need for individual review of each disclosure. For non-routine, non-recurring disclosures or requests for disclosures, covered entities must develop criteria to limit disclosures to the minimum necessary information while meeting the need of the disclosure request. They must also review each of these requests individually, following the established criteria (OCR, 2022).

Reasonable Reliance

Should another covered entity request PHI, a covered entity may rely on the request as complying with this minimum necessary standard if the request is reasonable under the circumstances. A covered entity may rely on requests as being the minimum necessary protected health information from:

- a public official
- a professional (attorney or accountant) who is a business associate of the covered entity seeking information to provide services to or for the covered entity
- a researcher who provides the documentation or representation required by the Privacy Rule for research (OCR, 2022).

Notice & Individual Rights

Privacy Practice Notice

All covered entities are required to provide a notice of their privacy practices. The notice must contain specific elements per the Privacy Rule. The notice must:

- Describe the ways the covered entity may use and disclose protected health information.
- State the duty to protect privacy, provide a notice of privacy practices, and follow the current terms required of the covered entity.
- Describe the individuals' rights, including the right to complain to the covered entity and to HHS if they suspect a violation of their privacy rights.
- Include contact details for the covered entity regarding additional information and procedures for making complaints.

Covered entities must follow their privacy practice notices. The Privacy Rule has specific requirements for the distribution of the notice for direct treatment providers, other healthcare providers, and health plans. The Department of Health and Human Services provides a model of the notice of privacy practices to help providers improve patients' experiences and knowledge. An example of one such model can be found in Appendix A. The notice of privacy practice can be used as is or modified to meet one's practice needs or state law requirements.

Notice Distribution

A healthcare provider with a direct treatment relationship with individuals must distribute a privacy notice to patients as described below:

- By personal delivery no later than the first service encounter (for patient visits), by an automatic and synchronous electronic response (for virtual service delivery), and by prompt mailing (for telephone service delivery).
- The notice must be posted at each service delivery location in a clear and prominent place, where individuals seeking service may reasonably be expected to be able to read the notice.

- In emergency treatment situations, the covered entity must provide its notice as soon as possible after the emergency concludes.

Covered entities, direct and indirect treatment providers, or health plan representatives must provide a notice to anyone who requests it. If a covered entity maintains a website for customer service or benefits information, the notice must be available on its website.

Covered entities in an organized healthcare arrangement can use a joint privacy practices notice as long as each party agrees to comply with the notice regarding PHI created or received as part of their participation in the joint arrangement. Any covered entity involved in the organized health care arrangement, which is the first point of contact with an OHCA member, is required to provide the joint privacy notice, which then satisfies the distribution requirement for all other covered entities in the OHCA.

Health plan representatives must issue a privacy practices notice to all new enrollees at the time of enrollment and provide a reminder to each enrollee every three years that the notice is available upon request.

Acknowledgment of Notice Receipt

A covered healthcare provider who administers direct treatment to individuals must make a good faith effort to acquire written acknowledgment from patients of receipt of the privacy practices notice. Should the provider fail to obtain the patient's written acknowledgment of receipt of the notice, the provider must document the reason. The provider is relieved of needing acknowledgment in an emergency treatment situation (OCR, 2022).

Case Example

A mental health outpatient center did not provide a notice of privacy practices to parents or their minor child, who was a patient at the center. During the Office of Civil Rights' investigation, the center admitted that it had not provided the parent or child with a notice before the mental health evaluation. To correct this situation, the mental health center's intake assessment policy and procedures were revised to specify that a notice of privacy practice is provided. Moving forward, the clinician will obtain a signed acknowledgment of receipt of the notice before the intake assessment. The acknowledgment form is now included in the intake packet. The mental health center also provided OCR with written assurance that all policy changes were brought to the attention of the staff involved in the child's care and then disseminated to all staff affected by the policy change (OCR, 2017).

Access

All persons have the right to review and receive a copy of their PHI in a covered entity's designated record set. A designated record set is the covered entity's collection of records. Such records are used to make decisions about an individual's treatment and include a provider's medical and billing records on individuals or a health plan's enrollment, case records, claims adjudication, payment, and medical management record systems.

The following protected health information is exempt from the Privacy Rule right to access:

- psychotherapy notes
- information collected for legal proceedings
- prohibited access to laboratory results by the Clinical Laboratory Improvement Act (CLIA)
- information held by certain research laboratories.

Covered entities may deny individuals the right to access their PHI in certain situations. One such example is when a healthcare provider believes access could cause harm to the patient or another person. In such circumstances, the individual has the right to have the denial reviewed by a licensed healthcare provider for a second opinion. Covered entities may access reasonable, cost-based fees for the cost of copying and postage (OCR, 2022).

Case Example

A patient alleged that his mental health provider, in private practice, failed to provide him access to his medical records. After OCR notified the provider of the allegation, the provider released the patient’s medical records and billed him $100.00 for a records review and an administrative fee. The Privacy Rule allows for charging a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. OCR followed up with the provider with the additional complaint. The provider resolved the matter by refunding the $100.00 fees (OCR, 2017).

Case Example

A complaint alleged that a mental health center refused to provide a patient with a copy of her medical record, including psychotherapy notes. OCR's investigation revealed that the mental health center allowed the patient to review her medical record, including the

psychotherapy notes, with her therapist. However, the mental health center did not provide the patient with a copy of her medical records. Covered entities are required by the Privacy Rule to allow patients access to their medical records and provide copies upon request; however, the Privacy Rule does exempt psychotherapy notes from this requirement. Although the mental health center personnel allowed the patient to review her medical record, this did not void their obligation to provide the complainant with a copy of her records. Corrective action taken included the mental health center providing the complainant with a copy of her medical record (except for psychotherapy notes) and revising its policies and procedures to ensure timely access to all individuals (OCR, 2017).

Amendment

Individuals have the right to request that covered entities amend their PHI in a designated record set should the information be incomplete or inaccurate. When a covered entity completes an amendment request, it should make reasonable efforts to provide the amendment to those the patient has identified as needing it. They should also provide the amendment to persons the covered entity knows may rely on the information to the detriment of the patient. If the covered entity denies the request, its representative must provide the patient with a written denial and allow the patient to submit a statement of disagreement to be included in the record. A covered entity must make amendments to the PHI in its designated record set upon receiving a notice to amend from another covered entity (OCR, 2022).

Disclosure Accounting

Patients have the right to an accounting of the disclosures of their PHI by covered entities or their business associates. The maximum disclosure accounting period is six years immediately preceding the accounting request.

The Privacy Rule does not require disclosure accounting for the following:

- treatment, payment, or healthcare operations
- the individual or the personal representative
- notification of, or to, persons involved in an individual's health care, payment for health care, for disaster relief, or for facility directories
- an authorization

- a limited data set
- national security or intelligence purposes
- correctional institutions or law enforcement officials regarding inmates or individuals in lawful custody for certain purposes
- Incident to otherwise permitted or required uses or disclosures.

Accounting for disclosures to law enforcement officials or health oversight agencies may be temporarily suspended if the accounting disclosure would impact their activities or investigations (OCR, 2022).

Restriction Request

Individuals have the right to request a covered entity restrict the use and disclosure of their PHI for treatment, payment, or health care operations, disclosure to people involved in the patient's health care or payment for health care, or disclosure to notify family members or others regarding the patient's general condition, location, or even death. While a covered entity has no obligation or requirement to agree to a restriction request, a covered entity that does agree to the request must comply with the agreed restrictions, except to treat the individual in a medical emergency (OCR, 2022).

Confidential Communications Requirements

Covered healthcare providers and health plan administrators must allow for alternative means or locations of communication for the individuals to request to receive communications of PHI other than those that the covered entity usually utilizes. Individuals may request that the provider communicates with them through a specific alternative phone number or address. Individuals may also request that the provider send communications in a sealed envelope instead of a postcard.

Health plan representatives are expected to accommodate requests if the individual indicates that the disclosure of all or part of the PHI could endanger the individual. The health plan is not allowed to question the statement of endangerment by the individual. Any covered entity may make a condition of confidential communication compliance request on the individual to specify an alternative address or method of contact and make arrangements for how any payment will be handled (OCR, 2022).

Case Example

A patient alleged that a clinic disclosed protected health information when a clinic staff member left a message on the patient's home phone answering machine, and therefore failed to accommodate the patient's request that communications of PHI be made only on her mobile or work phones. In response, the clinic instituted several actions to achieve compliance with the Privacy Rule. The clinic took the following corrective actions to resolve the violation: retrained an entire department concerning the Privacy Rule requirements, provided specific training to clinic staff members whose job duties included leaving messages for patients and revised the department's patient privacy policy to clarify patient rights to accommodations of requests to receive communications of PHI by alternative means or at alternative locations (OCR, 2017)

Administrative Requirements

The Department of Health and Human Services recognizes that covered entities range from small providers to large multi-state health plans. Therefore, the Rule is intended to allow covered entities the flexibility and scalability to assess their needs and implement appropriate solutions for their organization. What is appropriate for one covered entity will depend on the covered entity's business, size, and resources.

Privacy Policies and Procedures

Covered entities are required to develop and implement written privacy policies and procedures that comply with the HIPAA Privacy Rule.

Privacy Personnel

Covered entities are required to have a designated privacy official who is responsible for its privacy policy and procedures development and implementation. They must also have a contact person or office who is responsible for providing information to individuals on the covered entity's privacy practices as well as procedures for receiving complaints.

Workforce Training and Management

Covered entities are required to train all members of their workforce on privacy policies and procedures necessary for them to carry out their job functions. Workforce members

include employees, volunteers, and trainees. A covered entity must have appropriate penalties and enforce them when members of their workforce violate their privacy policies and procedures or the Privacy Rule.

Mitigation

Covered entities are required to mitigate any harmful effect it learns was caused by the use or disclosure of PHI by its workforce or business associates in violation of their privacy policies and procedures or the Privacy Rule.

Data Safeguards

Covered entities are required to maintain 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 according to otherwise permitted or required use or disclosure. An example of such safeguards may include shredding documents containing PHI prior to disposing of them, securing medical records with a lock and key or passcode, and limiting access to keys or passcodes (OCR, 2022).

Case Example

A social worker at a medical center explained HIV testing procedures to a patient in the waiting room, leading to the disclosure of protected health information in front of several other individuals. While completing their investigation, OCR personnel found computer screens at the medical center displaying patient information that were easily visible to patients. As a result, OCR required the medical center to establish policies and procedures for administrative and physical safeguards related to the communication of protected health information. The medical center trained all staff on the newly developed policies and procedures as part of their corrective actions. In addition, OCR required the medical center to reposition its computer monitors to prevent patients from viewing information on the screens. The center also installed computer monitor privacy screens to prevent impermissible disclosures (OCR, 2017).

Complaints

Covered entities are required to have procedures that enable individuals to file complaints about the entity’s compliance with privacy policies and procedures and the Privacy Rule.

The covered entity must explain its procedures in its privacy practices notice. Covered entities must identify to whom individuals can submit complaints at the covered entity and inform individuals that complaints can also be made to the Secretary of HHS.

Retaliation and Waiver

Covered entities may not retaliate against individuals for:

- exercising their rights established by the Privacy Rule
- assisting in an investigation by HHS or another legal authority
- opposing an act or practice that they believe violates the Privacy Rule.

Covered entities can not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, enrollment, or benefits eligibility (OCR, 2022).

Documentation and Record Retention

Covered entities must maintain, for six years after the last date of their creation or last effective date:

- privacy policies and procedures
- privacy practices notices
- disposition of complaints
- any other actions, activities, and designations that the Privacy Rule requires to be documented

Fully-Insured Group Health Plan Exception

A fully-insured group health plan that only maintains enrollment data and summary health information is obligated to comply with the ban on waiving individual rights and retaliatory acts and documentation requirements concerning plan documents under limited circumstances. Specifically, this occurs only if they are amended to allow for disclosure of PHI to a plan sponsor by a health insurance issuer or an HMO that services the group health plan (OCR, 2022).

Organizational Options

The Rule contains provisions that address various organizational issues that may affect the implementation of privacy protections.

Hybrid Entity

The Privacy Rule allows a covered entity to identify as a hybrid entity if it is a single legal entity that conducts both covered and non-covered functions. To be designated a hybrid entity, the covered entity must identify in writing its operations that perform covered functions as healthcare components. After making this designation, most of the Privacy Rule's requirements will apply only to the healthcare components. A covered entity not making this designation is subject to the Privacy Rule.

Affiliated Covered Entity

Legally separate covered entities affiliated with common ownership or control may designate themselves, in writing, as a single covered entity to comply with the Privacy Rule. However, an affiliated covered entity that performs multiple covered functions must operate each different covered function in compliance with the Privacy Rule provisions applicable to those specific functions.

Organized Health Care Arrangement

The Privacy Rule recognizes relationships between participating covered entities who share protected health information to manage and benefit their joint operations as organized health care arrangements. For example, covered entities in an OHCA can share PHI with each other for the arrangement's joint healthcare enterprises.

Covered Entities With Multiple Covered Functions

Covered entities that perform multiple covered functions must operate each of these functions in compliance with the Privacy Rule provisions applicable to its covered functions. For example, the covered entity can not use or disclose the PHI of an individual who receives services from one covered function for another covered function if the individual is not involved with both functions.

Group Health Plan Disclosures to Plan Sponsors

Group health plans, health insurers, or HMOs offered by the plan may disclose the following PHI to the plan sponsor:

- Enrollment or disenrollment information concerning the group health plan, a health insurer, or HMO offered by the plan.
- Summary health information, if requested by the plan sponsor, for the plan sponsor to receive premium bids to provide health insurance coverage through the group health plan or to adjust, amend, or end the group health plan. Summary health information summarizes claims history, claims expenses, or types of claims experiences of the individuals for whom the plan sponsor has provided health benefits through the group health plan. The information is stripped of all individual identifiers other than five-digit zip codes.
- The group health plan's enrollees' PHI for the plan sponsor's completion of administrative functions of the plan. The plan must receive documentation from the plan sponsor that the group health plan documents have been amended to restrict the plan sponsor's use and disclosure of protected health information. These restrictions must include statements that the plan sponsor will not use or disclose the PHI in connection with any other benefit plan or for any employment-related action or decision (OCR, 2022).

Case Example

A hospital employee's supervisor accessed the employee’s medical record in the hospital's electronic medical record system. OCR's investigation confirmed the supervisor had used and disclosed the employee's protected health information without the authorization by the employee to do so, nor was there any other Privacy Rule permitted access. Although employment records held by a covered entity in its role as an employer are not protected by the Privacy Rule, employees' medical records are protected. Corrective actions taken by the hospital to resolve the specific issues in the case included a letter of reprimand in the supervisor's personnel file, the supervisor receiving additional training about the Privacy Rule, and the hospital providing professional counsel to the supervisor about the appropriate use of the medical information of a subordinate (OCR, 2017).

Personal Representatives and Minors

Personal Representatives

Covered entities are required to treat a personal representative the same as the individual concerning the uses and disclosures of the individual's PHI and the individual's rights under the Privacy Rule. A personal representative is that individual who has been legally authorized to make health care decisions on the individual's behalf or to act for the deceased individual or estate. An exception allowed by the Privacy Rule is if a covered entity has a reasonable basis to believe that the personal representative may be abusing or neglecting the individual or that acknowledging the personal representative's request could endanger the individual (OCR, 2022).

Minors

Parents are usually the personal representatives of their minor children. Typically, parents can exercise individual rights on behalf of their minor children, such as access to medical records. However, there are exceptional cases where the parent would not be considered the personal representative. For these situations, the Privacy Rule defers to State laws and other regulations to determine the rights of parents to access and control their children's protected health information. If State and other laws are silent concerning parental access to the minor's PHI, it is at the covered entity's discretion to provide parents access to their minor child's health information or deny the request. The decision must be made by licensed healthcare providers exercising their professional judgment (OCR, 2022).

State Laws

In most cases, State laws contrary to the Privacy Rule are overruled by federal law and federal requirements will apply. Contrary is defined as the impossibility of the covered entity to comply with a State law, or if federal law and/or State law creates an obstacle to complying with the full purposes and objectives of the provisions of HIPAA.

Exceptions provided for in the Privacy Rule regarding the general rule that federal law preempts contrary State laws are:

- Regarding individually identifiable health information privacy and allows for greater privacy protections or rights concerning the information
- Reporting of child abuse, disease or injury, birth, death, or for public health monitoring, investigation, or intervention

- Requirements for certain health plan reporting, such as management or financial audits.

Exception Determination

In response to a request from a State, covered entity, or individual, preemption of contrary State law will not occur if HHS determines that the State law:

- Is required to prevent fraud and abuse related to the provision of health care or health care payment.
- Is required to ensure the State regulation of insurance and health plans to the expressed extent authorized by statute or regulation.
- Is required for the State to report on health care delivery or costs.
- Is required for purposes of serving public safety, health, or welfare. If a Privacy Rule provision is in contention, the Secretary determines if the privacy intrusion is justified when balanced against the need to be served.
- The regulation of the manufacturing, registration, distribution, dispensing, or other control of any controlled substances that is deemed a controlled substance by the State law (OCR, 2022).

Case Example

A private practice failed to honor a parent's request for a copy of her minor son's complete medical record. OCR's investigation found that the private practice had followed its state regulation that allows for a covered entity to provide a summary of the record instead of the complete record. OCR also provided technical assistance to the private practice, including an explanation that the Privacy Rule allows a covered entity to offer such a summary only if the person making the request agrees in advance to receive a summary rather than the complete record. Among the corrective actions to resolve the specific issues in the case, OCR required the private practice to revise its policy, and the private practice forwarded the parent a complete copy of her son's medical record (OCR, 2017).

Enforcement and Penalties for Noncompliance

Compliance

The Standards for Privacy of Individually Identifiable Health Information establishes a set of national standards for the use and disclosure of an individual's protected health information by covered entities and standards for individuals' privacy rights, including their understanding and control of how their health information is used. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, and they conduct compliance reviews and complaint investigations.

OCR will attempt to achieve compliance with the Privacy Rule by encouraging cooperation with the covered entities, and OCR may offer technical assistance to help the covered entities voluntarily comply with the Privacy Rule. Covered entities who fail to voluntarily comply with the standards may be subject to civil money penalties. In addition, certain Privacy Rule violations may lead to criminal prosecution (OCR, 2022).

Civil Money Penalties

OCR may impose a penalty on a covered entity for a failure to comply with a Privacy Rule requirement. Penalties can vary greatly depending on factors such as the violation date, if the covered entity knew of the failure to comply or should have known, or if the failure to comply by the covered entity was due to willful neglect. Penalties for multiple violations of the identical Privacy Rule requirement in a calendar are limited.

A penalty will not be imposed for violations in certain circumstances, including:

- The failure to comply was not due to willful neglect and was corrected within 30 days of the entity knowing the failure to comply had occurred (the time period can be extended at the discretion of OCR)
- The Department of Justice has already imposed a criminal penalty for failure to comply.

OCR has the discretion to decrease a penalty if the failure to comply was due to reasonable cause, or if, given the extent of the non-compliance, the penalty would be excessive. Prior to OCR imposing a penalty, the covered entity will be notified and provided with an opportunity to present written evidence of the circumstances that would reduce or prevent a penalty. The written evidence must be submitted to OCR within 30 days of receipt of the

notice. If OCR imposes a penalty, the covered entity has the right to an administrative hearing to appeal the imposed penalty (OCR,2022).

Case Example

The Department of Health and Human Services Office for Civil Rights imposed a penalty of $5.1 million on the health insurer Excellus Health Plan for a 2015 HIPAA violation where a data breach impacted 9.3 million individuals. In addition, data breaches occurred with Anthem (78.8 million records) and Premera Blue Cross. All three covered entities settled breach investigations with OCR and paid substantial financial penalties.

In the Excellus case, health plan representatives discovered hackers had gained access to their computer systems in August, 2015.. The breach investigation revealed that unauthorized access to its systems initially occurred in December 2013 and continued until May 2015. They reported the breach to OCR on September 9, 2015.

The hackers installed malware on Excellus's systems and accessed the healthcare data of millions of Excellus Health Plan members, including names, dates of birth, contact information, health plan ID numbers, Social Security numbers, claims data, financial account information, and clinical treatment information.

In June 2016, OCR began an investigation to determine if the breach was caused by the failure of Excellus Health Plan representatives to comply with HIPAA Privacy, Security, and Breach Notification Rules. The investigation identified five HIPAA rules and standards with which Excellus was potentially non-compliant.

OCR found that Excellus failed to conduct an accurate and thorough organization-wide risk analysis to identify risks and vulnerabilities to the confidentiality, integrity, and availability of the electronically protected health information (ePHI) of its members. They found sufficient measures had not been taken to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level. They also discovered that technical policies and procedures were insufficient which resulted in unauthorized persons and software programs being able to access systems containing ePHI. Since Excellus did not discover the system breach for over 18 months, 9,358,891 of its members were impacted. OCR also found that Excellus Health Plan lacked policies and procedures requiring regular information system activity reviews.

Excellus Health Plan agreed to the financial penalty with OCR to avoid further investigation and formal proceedings. The settlement was reached with no admission of liability or

wrongdoing. In addition to the financial penalty, Excellus was required to implement a corrective action plan that covered all areas of noncompliance identified by OCR during their investigation. Excellus also agreed to be monitored closely by OCR for two years to ensure continued compliance with the HIPAA Rules. OCR acknowledged the seriousness of these issues in the following statement: "Hacking continues to be the greatest threat to the privacy and security of individuals' health information," said OCR Director Roger Severino (Alder, 2021).

Criminal Penalties

In situations where the covered entity or business associate did not know about the violation, had followed reasonable diligence with protected health information, and would not have known they had violated a Privacy Rule, the entity could be fined between $100 and $50,000 for each violation and up to $1,500,000 if the same violation occurred multiple times in a calendar year. For violations due to reasonable cause but not due to willful neglect, the fine is a minimum of $1000, up to $50,000 per violation, and up to $1,500,000 for the same violation multiple times within a calendar year. For violations that were due to willful neglect but were corrected within 30-days of the covered entity or business associate becoming aware of the violation, the fine is a minimum of $10,000 and a maximum of $50,000 and up to $1,500,000 for the same violation multiple times within the calendar year. In situations where it is deemed the violation was due to willful neglect and the covered entity or business associate does not take corrective action within 30 days of becoming aware of the violation, the fine is a minimum of $50,000 per violation and up to $1,500,000 for the same violation multiple times within a calendar year. The fines can rise to $250,000 and up to 10 years imprisonment when the violation involves the intent to sell, transfer, or use identifiable health information for commercial purposes, personal gain, or malicious harm. Under the HIPAA Privacy Rule, the Justice Department is responsible for criminal prosecution (OCR, 2022 & eCFR, 2022).

Case Example

A patient care coordinator at the University of Pittsburgh Medical Center received a 1-year jail term for accessing the medical records of patients and using the information for malicious harm.

The coordinator accessed patients' medical records without authorization. She accessed the records of friends, old classmates, and individuals with whom she had grievances, and she then used the information from the medical records in a vendetta against her former

employer, where she had been an office manager. She accessed the medical records of the woman who replaced her and disclosed gynecological information about the woman to her employer via voicemail. The previous employer informed the Pittsburgh Medical Center, and the patient care coordinator was terminated. She was then hired by Allegheny Health Network, where she continued to access patient records without authorization. In total, she accessed 111 patients' records without authorization.

While she took some responsibility for her actions, she claimed she was going through a difficult time with health issues and that she was not aware she was breaking the law. Prosecutors argued she had been provided with HIPAA training and therefore was aware she was breaking the law and sought a jail term of six to twelve months. The judge found the crimes were egregious and sentenced her to twelve months in jail, with three years probation. In addition, she was not to contact any of the 111 victims (Alder, 2019).

Conclusion

The Health Insurance Portability and Accountability Act is a federal law establishing national standards to protect patient health information from being disclosed without patients' knowledge or consent. The Privacy Rule sets national standards for safeguarding individually identifiable health information and establishes procedures for the use and disclosure of protected health information by covered entities. It also establishes standards for individuals to better understand their health information and control its use. All healthcare providers are responsible for understanding what information is protected, implementing HIPAA requirements, and complying with the Privacy Rule.

References

Alder, S. (2021). Excellus Health Plan Settles HIPAA Violation Case and Pays $5.1 Million Penalty. HIPAA Journal. Retrieved December 2022. https://www.hipaajournal.com/excellus-health-plan-settles-hipaa-violation-case-and-pays-5-1-million-penalty/

Alder, S. (2019). Patient Care Coordinator Gets 1 Year Jail Term for HIPAA Violation. HIPAA Journal. Retrieved December 2022. https://www.hipaajournal.com/patient-care-coordinator-gets-1-year-jail-term-for-hipaa-violation/

Center for Disease Control and Prevention (CDC) (2022). Health Insurance Portability and Accountability Act of 1996 (HIPAA).Retrieved December 2022. https://www.cdc.gov/phlp/publications/topic/hipaa.html#security-rule

Code of Federal Regulations (eCFR) (2022). Title 45. Subtitle A. Subchapter C. Part 160. Retrieved December 2022. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160#

The Centers for Medicare & Medicaid Services (CMS) (2022). Transactions Overview. Retrieved December 2022. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview

Health and Human Services (2022). Model Notice of Privacy Practice. Retrived December 2022 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices

Office for Civil Rights (OCR). (2022). Summary of the HIPAA Privacy Rule. Retrieved December 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Office for Civil Rights (OCR). (2019). Business Associates. Retrieved December 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Office for Civil Rights (OCR) (2017). HIPAA Compliance & Enforcement Case Examples. Retrieved December 2022. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases

Appendix A: Notice of Privacy Practice

Health and Human Services Model Notice of Privacy Practice

Retrieved December 2022:

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

Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

Your Rights

You have the right to:

- Get a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

Your Choices

You have some choices in the way that we use and share information as we:

- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care

- Market our services and sell your information
- Raise funds

Our Uses and Disclosures

We may use and share your information as we:

- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.

- We may say “no” to your request, but we’ll tell you why in writing within 60 days.

Request confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say “yes” to all reasonable requests.

Ask us to limit what we use or share

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say “no” if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say “yes” unless a law requires us to share that information.

Get a list of those with whom we’ve shared information

- You can ask for a list (accounting) of the times we’ve shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We’ll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated

- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:

- We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures

How do we typically use or share your health information?

We typically use or share your health information in the following ways.

Treat you

We can use your health information and share it with other professionals who are treating you. Example:

A doctor treating you for an injury asks another doctor about your overall health condition.

Run our organization

We can use and share your health information to run our practice, improve your care, and contact you when necessary. Example: We use health information about you to manage your treatment and services.

Bill for your services

We can use and share your health information to bill and get payment from health plans or other entities.

Example: We give information about you to your health insurance plan so it will pay for your services.

How else can we use or share your health information?

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues

We can share health information about you for certain situations such as:

- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Do research

We can use or share your information for health research.

Comply with the law

We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

Respond to organ and tissue donation requests

We can share health information about you with organ procurement organizations.

Work with a medical examiner or funeral director

We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests

We can use or share health information about you:

- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions

We can share health information about you in response to a court or administrative order, or in response to a subpoena.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.

- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you.

The new notice will be available upon request, in our office, and on our website.

Other Instructions for Notice

- Insert Effective Date of this Notice
- Insert name or title of the privacy official (or other privacy contact) and his/her email address and phone number.
- Insert any special notes that apply to your entity's practices such as "we never market or sell personal information."
- The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.
- If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.
- If your entity is part of an OHCA (organized health care arrangement) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment, and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."