

A photograph of a smiling female healthcare provider with short grey hair and round glasses, wearing a white lab coat over a light blue patterned shirt. She is sitting at a desk, holding a clipboard and pen. The background is a bright, out-of-focus indoor setting with greenery visible through a window. The left side of the image has a blue overlay with a faint pattern.

Washington State **Confidentiality Toolkit for Providers**

Contents

Table of Contents	2	Breach Notification Rule	13
Disclaimer	3	What is a breach?.....	13
Introduction	4	Notification Requirements.....	13
Federal Confidentiality Laws	5	42 CFR Part 2	14
Privacy Rule	5	Washington State Health Care Privacy Laws	15
PHI.....	5	Uniform Health Care Information Act	
Covered Entities.....	5	(RCW 70.02).....	15
Business Associates.....	5	Health Care Information	15
Business Associate Agreements	6	Allowable Uses & Disclosures	15
HIPAA Defined Identifiers	6	Confidentiality Laws for Minors in Washington...	15
Minimum Necessary Standard	6	WA minor consent laws	16
Permitted Uses and Disclosures	7	Authorization Elements	17
Authorization	8	Mental Health and Sexually Transmitted Disease	
Uses and Disclosures Where Authorization is		(STD) records in Washington	17
Required	8	STDs – Permitted and Mandatory Disclosures	
Uses and Disclosures with Opportunity to Agree or		(RCW 70.02.220)	17
Object.....	9	Mental Health – Permitted and Mandatory	
Uses and Disclosures where Opportunity to Agree		Disclosures (RCW 70.02.230)	18
or Object is Not Required	9	Breach Notification under Washington State Law	
Notice of Privacy Practices	11	(RCW 42.56.590 & 19.255.010)	19
Individual Rights under HIPAA.....	11	What is Personal Information?	19
Security Rule.....	12	Notification Obligation.....	19
Administrative Safeguards	12	Attorney General Notification	20
Physical Safeguards.....	12	Timing of Notification	20
Technical Safeguards	12	When also subject to HIPAA	20
Organizational Requirements.....	13		

This document is for informational purposes only, is non-binding, and should not be construed as legal advice from Washington State or the Health Care Authority (HCA). Compliance with and interpretation of health care privacy laws is complex. Readers are encouraged to consult an attorney prior to operationalizing policies and procedures that control the use and disclosure of protected information.


HCA makes no warranties, express or implied, regarding errors or omissions and assumes no legal liability or responsibility for loss or damage resulting from the use of information included in this document.

Regulations for confidentiality of health records are subject to change. As a result, be sure to use this resource in conjunction with a review of current laws in case there have been updates since this resource was published.

Introduction

This toolkit is designed to clarify the state and federal laws that govern protected health information, and it is intended to increase the common level of understanding in Washington's health care community.

Confidentiality protections encourage individuals to seek the health care they need with the knowledge that their sensitive information will be protected. State and federal laws require certain entities, such as health care providers and health plans, to protect individually identifiable health information, and only disclose that information when allowed by law.

This resource is intended to provide a summary of state and federal confidentiality laws regarding information related to an individual's health care, particularly the Health Insurance Portability and Accountability Act (HIPAA), RCW 70.02, RCW 42.56.590 and RCW 19.255.010. 42 CFR Part 2 is another important federal law pertaining to substance use disorder health information, but is covered in [**HCA's Sharing Substance Use Disorder Information Guidance**](#) .

Federal Confidentiality Laws

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to encourage the development of the health information system and tasked the U.S. Department of Health and Human Services (HHS) with providing recommendations on standards for protected health information. In 2000, HHS issued a final rule, known as the Privacy Rule, and later published the Security Rule. In 2009, Congress passed the Health Information for Economic and Clinical Health Act in response to the growth of distinct digital record formats and storage systems, which significantly revised HIPAA. In 2013, HHS amended the Privacy Rule as part of a broad set of new regulations, referred to as the Omnibus Rule.

Privacy Rule

The Privacy Rule provides federal protections for individually identifiable health information held by covered entities (defined below) and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of individually identifiable health information with the patient's consent, or without consent in certain circumstances.

The Privacy Rule establishes a foundation of federal protections for the privacy of protected health information. In cases where multiple laws apply, the most restrictive law must be followed.

PHI

Protected Health Information (PHI) is health information collected from an individual, created or received by a covered entity that:

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; **and**
- Identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI can be maintained in an electronic or any other form. Certain records, like some educational records and employment records, are excluded from the definition of PHI.

Covered Entities

HIPAA establishes standards to protect PHI held by covered entities and their business associates. Covered entities are the following:

- Health Plan – A plan that provides or pays the cost of medical care. Includes Medicaid, Medicare, and self-funded plans.
- Health Care Provider – A provider of medical or health services (e.g., home health, hospitals, clinics) that transmits any health information in electronic form in connection with a HIPAA-covered transaction.
- Health Care Clearinghouses – Organizations that process health information on behalf of other organizations from a non-standard content into standard data elements or to a standard transaction (e.g., billing services, health information systems).

Business Associates

A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered entity can be a business associate of another covered entity. The Privacy Rule lists some of the services, functions, and activities that make a person or entity a business associate. Business associate functions and activities can include:


- Claims processing or administration
- Data analysis
- Processing or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Practice management
- Repricing.

Business associate services can include:

- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation
- Management
- Administrative
- Accreditation
- Financial
- See the definition of "business associate" at 45 CFR 160.103.


Examples of business associates:

- A third-party administrator that assists a health plan with claims processing
- A CPA firm whose accounting services to a health care provider involve access to PHI
- An attorney whose legal services to a health plan involve access to PHI
- A consultant that performs utilization reviews for a hospital
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer
- An independent medical transcriptionist that provides transcription services to a physician
- A pharmacy benefits manager that manages a health plan's pharmacist network

HHS guidance on business associates can be found [here](#) .

Business Associate Agreements

When a covered entity uses a contractor or other non-workforce member to perform “certain” services or activities, the Privacy Rule requires that the covered entity include certain protections for the information in a business associate agreement (BAA). In the BAA, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates. Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of PHI that would violate the Rule.

Sample BAA language is available on the OCR website [here](#) .


HIPAA Defined Identifiers

Many common identifiers can be considered PHI, including:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the U.S. Census Bureau:
 - a. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and

- b. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000

3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Vehicle identifiers and serial numbers, including license plate numbers
6. Fax numbers
7. Device identifiers and serial numbers
8. Email addresses
9. Web Universal Resource Locators (URLs)
10. Social security numbers
11. Internet Protocol (IP) addresses
12. Medical record numbers
13. Biometric identifiers, including finger and voice prints
14. Health plan beneficiary numbers
15. Full-face photographs and any comparable images
16. Account numbers
17. Any other unique identifying number, characteristic, or code, except as permitted
18. Certificate/license numbers

HHS guidance on these identifiers and methods for de-identification can be found [here](#) .

Minimum Necessary Standard


As described below, a covered entity may disclose PHI under certain circumstances. These disclosures are typically subject to the “minimum necessary standard.” The minimum necessary standard, a key protection of the 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. Put another way, only the minimum amount of PHI necessary to carry out a function should be used or disclosed.

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

- Disclosures to or requests by a health care 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 HIPAA Administrative Simplification Rules
- Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses or disclosures that are required by other law

A covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, PHI for payment and health care operations to the minimum necessary. A covered entity also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to PHI for treatment, payment, and health care operations, based on those who need access to the information to do their jobs. Business associates must also abide by the minimum necessary standard.

HHS guidance on the minimum necessary standard can be found [here](#) .

Permitted Uses and Disclosures

The Privacy Rule generally prohibits a covered entity from using or disclosing PHI unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities.

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


- To the individual (unless required for access or accounting of disclosures)
- Treatment, payment, and health care operations
- Certain situations where the individual is given an opportunity to agree or object
- Situations incident to an otherwise permitted use and disclosure
- Public interest and benefit activities
- Limited data sets for the purposes of research, public health, or health care operations

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

To the Individual

The Privacy Rule generally requires a covered entity to provide individuals with access to PHI about them upon request. This includes the right to inspect or obtain a copy of the PHI (or both), as well as to direct the covered entity to transmit a copy to a designated person or entity. The minimum necessary standard does not apply to disclosures made to the individual about their own PHI.

When an individual makes a request for their PHI, a covered entity must provide access to the PHI requested in whole or in part (if certain access may be denied as explained below) no later than 30 calendar days from receiving the individual's request. See 45 CFR 164.524(b)(2). The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible. If a covered entity is unable to provide access within 30 calendar days—for example, where the information is archived offsite and not readily accessible—the covered entity may extend the time by no more than an additional 30 days. To extend the time, the covered entity must, within the initial 30 days, inform the individual in writing of the reasons for the delay and the date by which the covered entity will provide access. Only one extension is permitted per access request.

HHS guidance on individuals' right to access their own PHI under HIPAA can be found [here](#) .

Treatment, Payment, and Health Care Operations

The Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for:

- **Treatment** – The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another;
- **Payment** – The various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care; and
- **Health Care Operations** – Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

Ready access to treatment and efficient payment for health care, both of which require use and disclosure of PHI, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers

and health plans are essential to support treatment and payment. To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for treatment, payment, and health care operations activities.

HHS guidance on disclosures for treatment, payment, and operations can be found [here](#).

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," as required by the Privacy Rule.

HHS guidance on incidental use and disclosure can be found [here](#).

Authorization

A covered entity **must** obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. An authorization must be written in specific terms. The core elements of a valid authorization include:

- A meaningful description of the information to be disclosed.
- The name of the individual or entity authorized to make the requested disclosure.
- The name of the recipient of the information
- A description of each purpose of the disclosure (The statement "at the request of the individual" is sufficient when the individual initiates the authorization and does not, or elects not to, provide a statement of the purpose)
- An expiration date or an expiration event that relates to the individual
- A signature of the individual or their personal representative and the date.

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
- Disclosures to a pharmaceutical firm for their own marketing purposes.

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, and the right to revoke in writing.

Uses and Disclosures Where Authorization is Required

Psychotherapy Notes

A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

- The covered entity who originated the notes may use them for treatment.
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for 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 or as required by law.

The Privacy Rule defines psychotherapy notes specifically as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record."

The definition of psychotherapy notes expressly excludes specific types of information that might otherwise be included in service/progress notes, including "medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." See 45 CFR 164.501.

According to HHS, "Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that

typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes.”

More guidance from HHS on mental health information and psychotherapy notes can be found [here](#) and [here](#).

Marketing

Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. Any disclosure of PHI for marketing purposes requires patient authorization. However, the Privacy Rule excludes the following health-related activities from this definition of marketing:

- 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; and
- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

Uses and Disclosures with Opportunity to Agree or Object

In some circumstances, a covered entity may disclose PHI, but the individual must be informed in advance and given an opportunity to agree, prohibit or reject the disclosure. A covered entity may orally inform the individual of and obtain the individual’s oral agreement or objection. The circumstances where PHI can be disclosed are:

1. Maintaining facility directories
 - a. A covered health care 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.
 - b. 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.
 - c. If the individual is incapacitated or in an emergency,

a covered entity may disclose PHI if, in the exercise of their best professional judgment, it is determined to be in the best interests of the individual and is consistent with the prior expressed interest of the individual.

2. For notification and other purposes: a covered entity may disclose to the individual’s family, relatives, or friends, or to other persons whom the individual identifies, PHI directly relevant to that person’s involvement in the individual’s care or payment for care, provided that:
 - a. the individual is present and either agrees to the disclosure or is given an opportunity to object and does not expressly do so;
 - b. if the individual is not present, during an emergency circumstance, or the individual is incapacitated, the disclosure is in the best interests of the individual’s care or related payment; or
 - c. the individual is deceased and such persons receiving the PHI were involved in the individual’s care or payment and such disclosure is relevant to the person’s involvement.
3. Additionally, PHI may be disclosed for notification purposes to public or private entities authorized by law to assist in disaster relief efforts.

Uses and Disclosures where Opportunity to Agree or Object is Not Required

The Privacy Rule permits use and disclosure of PHI, without an individual’s authorization or permission, for twelve 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.

1. Required by Law

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

2. Public Health Activities

The Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals.

Accordingly, the Rule permits covered entities to disclose PHI without authorization for specified public health purposes.

Covered entities may disclose PHI to:

- 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 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; and
- 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 (MSHA), or similar state law.

HHS guidance on disclosures for public health activities can be found [here](#).

3. 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.

4. Health Oversight Activities

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

5. 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.

6. Law Enforcement Purposes

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

- 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; and
- By a covered health care 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.

7. 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.

8. 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.

9. Research

The Privacy Rule establishes the conditions under which PHI may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See 45 CFR 164.501. A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with 45 CFR 164.502(d), and 164.514(a)-(c) of the Rule). In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule. 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:

- 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; or
- 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

Read HHS guidance on disclosing PHI for research purposes [↗](#).

10. 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.

11. Essential Government Functions

An authorization is not required to use or disclose PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, 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, and determining eligibility for or conducting enrollment in certain government benefit programs.

12. 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.

Read HHS guidance on disclosures for workers' compensation purposes [↗](#).

Limited Data Set

A limited data set 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, health care 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.

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. The notice must state the covered entity's duties to protect privacy, provide of the covered entity's privacy practices, and that the covered entity will abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to 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 of notices for direct treatment providers, all other health care providers, and health plans.

Read HHS guidance on notice of privacy practices [↗](#).

Individual Rights under HIPAA

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.

Amendment

The Privacy Rule gives individuals the right to have covered entities amend their PHI in a designated record set when that information is inaccurate or incomplete.

Accounting of Disclosures

Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates.

Restriction Request

Individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment or health care 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.

Confidential Communication Requirements

Health plans and covered health care 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.

HHS guidance on individuals' right to access their own PHI under HIPAA can be found [here](#).

Security Rule

The HIPAA Security Rule requires covered entities to have security measures in place 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. The Security Rule requires covered entities to develop reasonable and appropriate security policies. In addition, covered entities must analyze security risks in their environment and create appropriate solutions. What's reasonable and appropriate depends on business size, complexity, and resources. Covered entities must:

- Ensure the confidentiality, integrity, and availability of all PHI created, received, maintained, or transmitted
- Identify and protect against threats to PHI security or integrity
- Protect against impermissible uses or disclosures
- Ensure employee compliance. When developing compliant safety measures, consider:
 - Size, complexity, and capabilities of the organization
 - Technical, hardware, and software infrastructure
 - The costs of security measures
 - The likelihood and possible impact of risks to PHI

Visit the [HHS HIPAA Guidance Materials webpage](#) and [Summary of the HIPAA Security Rule webpage](#) for guidance on:

- Administrative, physical, and technical PHI safety measures
- Cybersecurity
- Remote and mobile use of PHI

Administrative Safeguards

The Security Rule defines administrative safeguards as “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI

and to manage the conduct of the covered entity's workforce in relation to the protection of that information.” This includes the following standard measures:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation

[Read HHS guidance on administrative safeguards](#).

Physical Safeguards

The Security Rule defines physical safeguards as “physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” When evaluating and implementing these standards, a covered entity must consider all physical access to PHI. This may extend outside of an actual office, and could include workforce members' homes or other physical locations where they access PHI, including the following measures:

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

[Read HHS Guidance on physical safeguards](#).

Technical Safeguards

The Security Rule defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic PHI and control access to it.” The Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization. This includes the following measures:

- Access control
- Audit controls
- Integrity
- Personal or entity authentication
- Transmission security

[Read HHS guidance on technical safeguards](#)

Organizational Requirements

While the vast majority of standards and implementation specifications can be found in the administrative, physical and technical safeguards, covered entities must also follow certain organizational requirements to achieve compliance, including:

- BAAs or other arrangements (see page 5)
- Requirements for group health plans

HHS guidance on organizational requirements can be found [here](#). See also 45 CFR §§ 164.314-316.

Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires covered entities and their business associates to provide notification following a breach of PHI.

What is a breach?

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

- 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; and
- The extent to which the risk to the PHI has been mitigated.

Covered entities and business associates, where applicable, 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. There are three exceptions to the definition of “breach.”

1. 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.
2. 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 health care 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.

3. 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.

Notification Requirements

(**Note:** state laws have notification requirements as well. See page 27)

Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the HHS 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.

Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI. Covered entities must provide individual notice 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 web site 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 other means.

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, 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, as applicable).

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.

Visit the [HHS HIPAA Breach Notification Rule](#) webpage for guidance on:

- Administrative requirements and burden of proof
- How to make unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals
- Reporting requirements

42 CFR Part 2

Certain substance use disorder (SUD) treatment information is subject to stringent regulations in 42 Code of Federal Regulations (CFR) Part 2 (sometimes just referred to as “Part 2”). Part 2 only applies to SUD treatment information created by particular providers called Part 2 Programs. A provider that provides SUD services is a Part 2 Program if it holds itself out as offering SUD services and is federally assisted. The data these providers produce in their capacity as Part 2 Providers is called Part 2 data.

In cases where multiple laws apply, the most restrictive law must be followed.

Part 2 is not covered in this toolkit. For more information on Part 2, HCA has guidance available [here](#).

Washington State Health Care Privacy Laws

In cases where multiple laws apply, the most restrictive law must be followed.

Uniform Health Care Information Act (RCW 70.02)

Under Washington state law, health care information (HCI) is considered confidential. Confidentiality is considered to enhance open and honest communication between patients and their providers. The primary source for confidentiality and the requirements for the release of HCI in Washington is found in the Uniform Health Care Information Act 70.02 RCW (the “Act”), which Washington adopted in 1991.

The UHCIA provides confidentiality protection for medical records and patients’ HCI and requires consent in most cases for release of the records or disclosure of the information, subject to certain exceptions. Specific requirements govern confidentiality of information related to mental health services and sexually transmitted diseases. Many of the requirements of Washington law are parallel with the federal HIPAA Privacy Rule for disclosure of PHI, but include some stronger protections. Washington laws also contain provisions that are specific to the confidentiality of minors’ HCI, particularly with respect to parents’ access to that information.

Health Care Information

A health record is a compilation of HCI that identifies the patient, justifies the patient’s diagnosis and treatment, and documents the results of the patient’s treatment. Under the Act, the term “health care information” means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by HCA concerning a client or potential client; and (2) Relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and (3) Identifies or can readily be associated with the identity of a client or potential client. Just as PHI is a defined term in HIPAA, HCI is a defined term in the Act.

HCI serves a number of purposes. HCI is maintained primarily to provide accurate and complete information about the care and treatment of a patient. HCI enhances communication among the patient’s physician and other health care professionals treating the patient. Records also show the extent and quality of care for statistical, research and educational purposes and may be used for future review, study and evaluation of the care rendered to the patient. In addition, HCI provides information for billing and reimbursement. Finally, HCI is a valuable aid in legal proceedings.

Allowable Uses & Disclosures

A health care provider (including individuals who assist a health care provider in the delivery of health care, or an agent or employee of a provider) may not disclose HCI about a patient to any other person without an appropriate written authorization. Such an authorization may be given by a patient who is competent. In the case of an incompetent patient (as defined in RCW 11.88.010(1)), the person who is legally authorized to consent to health care for the patient under the Informed Consent Statute (RCW 7.70.065) may exercise the rights of the patient under the Act.

Confidentiality Laws for Minors in Washington

Generally, in the case of a minor patient, the patient’s HCI may be released only with the consent of the patient’s parent or legal guardian. However, a minor who is authorized by law to consent to health care without parental consent, may exercise the rights of the patient under the Act as to information pertaining to the health care to which the minor lawfully consented. In Washington, minors in the following categories may consent to treatment:

- emancipated minors;
- a minor married to a person over 18 years of age;
- a minor 14 years or older seeking treatment for sexually transmitted diseases;
- a minor 13 years or older seeking outpatient treatment for drug and alcohol abuse;
- a minor 13 years or older requesting outpatient treatment for mental illness;
- a minor under the age of eighteen to voluntary termination of pregnancy as long as the fetus is not viable; and
- a minor parent with sufficient capacity may consent to medical treatment for his/her child.

Accordingly, a minor may authorize the release of health care information in the above situations in the event that they consented to such treatment.

In cases where parental consent is required, a health care provider may rely, without incurring any civil or criminal liability for such reliance, on the representation of a parent that he or she is authorized to consent to health care for the minor patient, regardless of whether:

- the parents are married, unmarried, or separated,
- the consenting parent is or is not the custodial parent, or
- the consent is or is not in full performance of any agreement between the parents or an order or decree under RCW 26.09

WA minor consent laws

Service Needed	Parent/Guardian Consent Required?	Notes/Source
Emergency Medical Services	No, but only if parent's consent is not readily available	RCW 7.70.050(4); 18.71.220
Non-Emergency Medical Services	Yes, unless minor is a Mature Minor (see page 23) or is homeless	Smith v. Seibly, 72 Wn. 2d 16 (1967)
Immunizations	Yes, unless minor is a Mature Minor (see page 23)	Minors may receive immunizations without parental consent under mature minor doctrine.
Sexually Transmitted Disease (STD) testing/treatment	Yes, unless youth is 14 or older	RCW 70.24.110 Minors may obtain tests and/or treatment for STDs if they are 14 years of age or older without the consent of a parent or guardian.
Birth control services	No	RCW 9.02.100(1) Minors may obtain or refuse birth control services at any age without the consent of a parent or guardian.
Abortion services	No	RCW 9.02.100(2); State v. Koome, 530 P.2d 260 (1975) Minors may receive an abortion and abortion related services at any age without the consent of parent/guardian.
Prenatal care services	No	State v. Koome, 530 P.2d 260 (1975) Minors may seek prenatal care at any age without the consent of parent/guardian.
Outpatient mental health treatment	Yes, unless youth is 13 or older	RCW 71.34.500-530 Minors may receive outpatient mental health treatment if they are 13 years of age or older without the consent of parent/guardian.
Inpatient mental health treatment	Yes, unless youth is 13 or older	RCW 71.34.500-530 Minors 13 years of age or older may receive inpatient mental health treatment without parental consent. Parents must be notified.
Outpatient substance abuse treatment	Yes, unless youth is 13 or older	RCW 71.34.500-530 Minors 13 years of age or older may receive outpatient SUD tx, without parental consent.
Inpatient substance abuse treatment	Yes, unless child is determined to be a child in need of services	RCW 71.34.500-530 Minors 13 years of age or older may receive inpatient SUD tx without parental consent if DSHS determined child is in need of services.

Status	Minor Consent	Notes	Citations
Age of majority	< 18 — NO > 18 — YES	Age of majority is 18	RCW 26.28.010; 26.28.015
Emancipated minor	Yes	Emancipated minor may consent	RCW 13.64.060
Mature Minor	Yes	A minor may be considered emancipated for purpose of consenting to health care based on “age, intelligence, maturity, training, experience, economic independence or lack thereof, general conduct as an adult and freedom from the control of parents”	Smith v. Seibly, 72 Wn. 2d 16 (1967)
Married minor	Yes, with limitations	A minor married to an adult is considered an adult and would therefore be able to consent for health care.	RCW 26.28.020

Authorization Elements

The essential elements to a valid authorization to disclose health care information are:

1. the authorization must be in writing, dated and signed by the patient (or other legally authorized representative);
2. the authorization must identify the patient;
3. it must also identify the information to be disclosed;
4. the authorization must identify the name and institutional affiliation of the person or class of persons to whom the information is to be disclosed;
5. the authorization must identify the health care provider or class of providers making the disclosure; and
6. the authorization must contain an expiration date or an expiration event that relates to the patient or the purpose or use of the disclosure being authorized

A patient may revoke an authorization to disclose health care information in writing at any time unless the information is needed to process payment for health care that has already been provided or other substantial action has been taken in reliance on the authorization. A patient may not sue a health care provider for disclosures made in good-faith reliance on an authorization to release health records if the health care provider had no actual notice of the revocation of the authorization. A written authorization must meet the requirements of both state law and federal law, such as HIPAA and Part 2 as applicable.

Mental Health and Sexually Transmitted Disease (STD) records in Washington

Mental health and STD treatment records are treated separately from other health records under Washington law. Heightened standards of confidentiality beyond HIPAA and other state law are required when using or disclosing PHI

pertaining to STDs and mental health records, and there are very limited exceptions for which disclosure is permissible. Below is a summarized list of permitted exceptions to this rule:

STDs – Permitted and Mandatory Disclosures (RCW 70.02.220)

No person may disclose or be compelled to disclose information and records related to sexually transmitted diseases. A person may disclose information related to sexually transmitted diseases about a patient without the patient’s authorization, to the extent the recipient needs to know the information, if the disclosure is to:

- a. The subject of the test or the subject’s legal representative;
- b. State/local public health officer or the CDC;
- c. A health facility or health care provider;
- d. Any state or local public health officer conducting an investigation pursuant to RCW 70.24.024
- e. A person allowed access to the record by a court order granted after application showing good cause;
- f. Persons who, because of their behavioral interaction with the infected individual, have been placed at risk for acquisition of a sexually transmitted disease;
- g. A law enforcement officer, firefighter, health care provider, health care facility staff person, Department of Correction’s staff person, jail staff person, or other persons as defined by the board of health, who has requested a test of a person whose bodily fluids he or she has been substantially exposed to, if a state or local public health officer performs the test;
- h. Claims management personnel employed by or associated with an insurer, health care service contractor, health maintenance organization, self-funded health plan, state administered health care

claims payer, or any other payer of health care claims;
or

- i.** A Department of Children, Youth, And Families (DCYF) worker, a child-placing agency worker, or a guardian ad litem who is responsible for making or reviewing placement or case-planning decisions or recommendations to the court regarding a child, who is less than fourteen years of age, has a sexually transmitted disease, and is in the custody of DCYF or a licensed child-placing agency.

Mental Health – Permitted and Mandatory Disclosures (RCW 70.02.230)

Information and records related to mental health services, other than those obtained through treatment under RCW 71.34 (Behavioral Health Services for Minors), may be disclosed pursuant to a valid authorization or may be disclosed only:

- a.** In communication with qualified professionals;
- b.** When the communications regard the special needs of a patient and the necessary circumstances giving rise to such needs and the disclosure is made by a facility providing services to the operator of a facility in which the patient resides or will reside;
- c.** To a Guardian, next of kin, designated representative, etc;
- d.** To the Courts or when required by law;
- e.** Between mental health professionals and representatives in certain situations;
- f.** To the attorney of the detained person;
- g.** To the prosecuting attorney as necessary to carry out the responsibilities of the office;
- h.** To appropriate law enforcement agencies and to a person, when the identity of the person is known to the public or private agency, whose health and safety has been threatened, or who is known to have been repeatedly harassed, by the patient;
- i.** To appropriate corrections and law enforcement agencies all necessary and relevant information in the event of a crisis or emergent situation that poses a significant and imminent risk to the public;
- j.** To the persons designated in RCW 71.05.425 for the purposes described in those sections;
- k.** By a care coordinator under certain circumstances;
- l.** Upon the death of a person. The person's next of kin, personal representative, guardian, or conservator, if any, must be notified;
- m.** To mark headstones or otherwise memorialize patients interred at state hospital cemeteries.
- n.** To law enforcement officers and to prosecuting attorneys as are necessary to enforce RCW 9.41.040(2)(a)(iv);
- o.** When disclosure is necessary for the protection of the patient or others;
- p.** Pursuant to lawful order of a court, including a tribal court;
- q.** To qualified staff members of the Department of Social and Health Services (DSHS), to HCA, to behavioral health administrative services organizations, to managed care organizations, to resource management services responsible for serving a patient, or to service providers designated by resource management services as necessary to determine the progress and adequacy of treatment and to determine whether the person should be transferred to a less restrictive or more appropriate treatment modality or facility;
- r.** Within the mental health service agency or Indian health care provider facility where the patient is receiving treatment;
- s.** Within DSHS and HCA as necessary to coordinate treatment for mental illness, developmental disabilities, alcoholism, or substance use disorder of persons who are under the supervision of DSHS;
- t.** Between DSHS, DCYF, and HCA as necessary to coordinate treatment for mental illness, developmental disabilities, alcoholism, or drug abuse of persons who are under the supervision of the DSHS or the DCYF;
- u.** To a licensed physician or psychiatric advanced registered nurse practitioner to treat a medical emergency;
- v.** For care coordination purposes;
- w.** To administrative and office support staff designated to obtain medical records for certain licensed professionals;
- x.** To a facility that is to receive a person who is involuntarily committed under chapter 71.05 RCW, or upon transfer of the person from one evaluation and treatment facility to another;
- y.** To the person's counsel or guardian ad litem, without modification, at any time in order to prepare for involuntary commitment or recommitment proceedings, etc;
- z.** To staff members of the protection and advocacy agency or to staff members of a private, nonprofit corporation for the purpose of protecting and advocating the rights of persons with mental disorders or developmental disabilities;
- aa.** To all current treating providers, including Indian health care providers, of the patient with prescriptive authority who have written a prescription for the patient within the last twelve months;
- ab.** To the secretary of social and health services and the director of HCA for either program evaluation or

research, or both;

- ac.** To any person if the conditions in RCW 70.02.205 are met;
- ad.** To the Secretary of Health for the purposes of the maternal mortality review panel established in RCW 70.54.450; or
- ae.** To a tribe or Indian health care provider to carry out the requirements of RCW 71.05.150(7).

Breach Notification under Washington State Law (RCW 42.56.590 & 19.255.010)

Washington law requires businesses, individuals, and public agencies to notify any Washington resident who is at risk of harm because of the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of that resident's if it has determined that a breach of personal information has occurred. Any business, individual, or public agency that is required to issue a security breach notification to more than 500 Washington residents as a result of a single security breach must electronically submit a single sample copy, excluding any personally identifiable information, to the Washington State Attorney General.

The notification to affected consumers and to the Attorney General must be made in the most expedient time possible and without unreasonable delay, no more than 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

A covered entity under HIPAA is deemed to have complied with this law if it has complied with HIPAA breach notification requirements. Covered entities must still notify the Attorney General when applicable. (RCW 42.56.592 & 19.255.030)

What is Personal Information?

For purposes of this law, personal information includes:

- (1)** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - a.** Social security number or the last four digits of the social security number;
 - b.** Driver's license number or state identification card number;
 - c.** Account number, credit card number, or debit card number in combination with any required security

code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account.

- d.** Full date of birth;
- e.** Private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- f.** Student, military, or passport identification number;
- g.** Health insurance policy number or health insurance identification number;
- h.** Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or
- i.** Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

- (2)** Username or email address in combination with a password or security questions and answers that would permit access to an online account; and
- (3)** Any of the data elements or any combination of the data elements described in (1) above, without the consumer's first name or first initial and last name if:
 - a.** Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
 - b.** The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notification Obligation

Any entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of WA whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not "secured" (i.e., encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person).

Notice is not required if the breach of the security of the

system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

Attorney General Notification

Any entity that is required to issue a notification to more than 500 Washington State residents as a result of a single breach must, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. The entity must include the following information:

1. The number of Washington consumers affected by the breach, or an estimate if the exact number is not known;
2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
3. A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
4. A summary of steps taken to contain the breach.

The notice to the attorney general must be updated if any of the information identified above is unknown at the time the notice is due.

Timing of Notification

The disclosure to affected consumers and to the Attorney General must be made in the most expedient time possible, and no more than 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

When also subject to HIPAA

Covered entities (as defined by HIPAA) are deemed to have complied with the requirements of RCW 42.56 if they have complied with the breach notification requirements of HIPAA. Meaning, even though state law requires notification be made in 30 days, if HIPAA is applicable, HIPAA's 60-day requirement is deemed to be compliant with both laws.