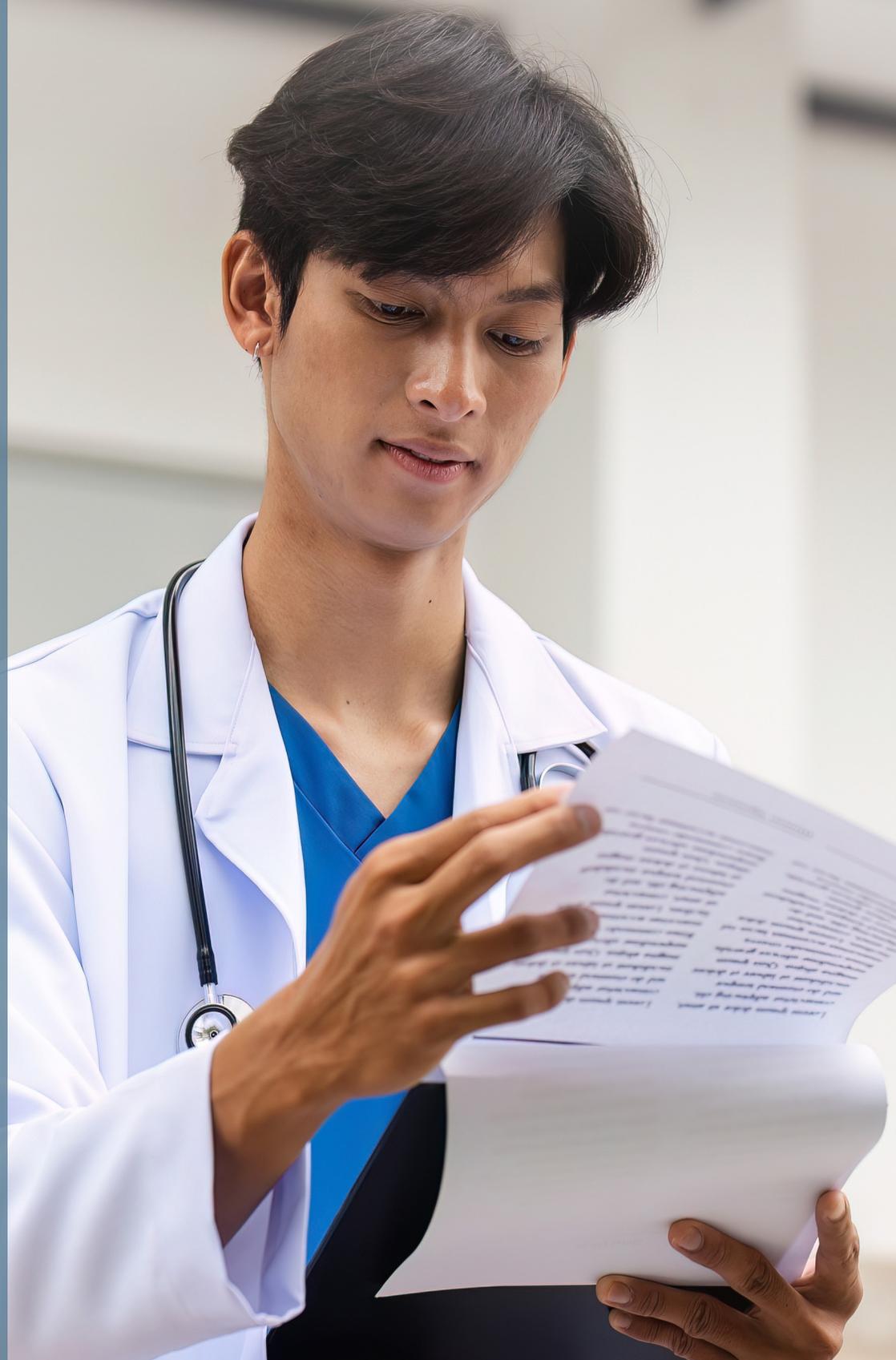


Washington Health Care Privacy Toolkit



Contents

Introduction	3	Breach Notification Rule	11
Disclaimer	3	What is a breach?	11
Privacy laws at-a-glance	4	Notification Requirements.....	12
Federal Confidentiality Laws	6	Substance use disorder treatment	12
Privacy Rule	6	Washington State Health Care Privacy Laws	13
Protected health information	6	Uniform Health Care Information Act	
HIPAA-defined identifiers	6	Health care information	13
Covered Entities	7	Allowable uses and disclosures.....	13
Business Associates.....	7	Confidentiality laws for minors in Washington....	13
Business Associate Agreements.....	7	Washington minor consent laws	14
Minimum necessary standard	7	Authorization Elements.....	15
Permitted uses and disclosures	8	Mental health and sexually transmitted disease (STD) records in Washington.....	15
Authorization.....	8	Breach notification under Washington State law	15
Uses and Disclosures Where Authorization is Required	8	Notification obligation.....	15
Psychotherapy notes.....	8	Attorney general notification.....	15
Marketing	9	Timing of Notification	15
Uses and Disclosures with Opportunity to Agree or Object.....	9	When also subject to HIPAA.....	16
Uses and Disclosures where Opportunity to Agree or Object is Not Required.....	9	Use of electronic signatures	16
Notice of Privacy Practices.....	10	2024 Updates to reproductive health privacy	17
Individual Rights under HIPAA.....	10	HIPAA Privacy Rule to Support Reproductive Health Care Privacy	17
Security Rule	11	Prohibition.....	17
Administrative Safeguards.....	11	Attestation.....	17
Physical Safeguards.....	11	Washington My Health My Data Act	17
Technical Safeguards.....	11		

Introduction

This toolkit discusses many of the state and federal laws that govern sensitive health information, and it is intended to assist 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 to only disclose that information when allowed by law.

This resource focuses on the Health Insurance Portability and Accountability Act (HIPAA) and related state law. 42 CFR (Part 2) is another important federal law pertaining to substance use disorder health information, and is covered in the Health Care Authority's (HCA) [Sharing Substance Use Disorder Information Guidance](#) .

Disclaimer

This document is for informational purposes only, is nonbinding, and should not be construed as legal advice from Washington State or HCA. Complying with 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 sensitive health 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.

Privacy laws at-a-glance

🔑 Law	📄 Summary	👤 Who must comply?	🔒 Protected information	✔️ Commonly used permitted disclosures
HIPAA 	<p>HIPAA is a national standard that protects sensitive patient health information from being disclosed without the patient’s consent or knowledge. The main goal is to ensure that people’s health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care.</p>	<ul style="list-style-type: none"> • Health care providers who electronically transmits health information in connection with certain transactions • Health plans • Health care clearinghouses • Business associates that act on behalf of a covered entity, including claims processing, data analysis, utilization review, and billing 	<p>Protected health information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.</p>	<ul style="list-style-type: none"> • To the individual • Treatment, payment, and health care operations • Research • Certain law enforcement purposes • In response to a serious threat to health and safety
42 CFR (Part 2) 	<p>The regulations at Part 2 protect the confidentiality of substance use disorder (SUD) treatment records.</p> <p>Confidentiality protections help address concerns that discrimination and fear of prosecution deter people from entering treatment for SUD.</p>	<ul style="list-style-type: none"> • Federally assisted programs that hold themselves out as providing substance use disorder diagnosis, treatment, or referral for treatment • Federally assisted includes (but isn’t limited to) receiving federal funds or receiving a federal license • Qualified service organizations (entities that perform services for a Part 2 Program) • Lawful holders (i.e., people who receive information and notice from Part 2 programs). 	<p>Part 2 protects records of the identity, diagnosis, prognosis, or treatment of any patient in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States.</p>	<ul style="list-style-type: none"> • Communications within Part 2 program for those who have a need to know • Medical emergency where a patient cannot consent • Report a crime or threats on Part 2 premises or against Part 2 personnel to law enforcement; limit information • Report child abuse or neglect • Research • Audit or evaluation of Part 2 program by a government, payer, or other lawful holder; subject to conditions
FERPA 	<p>The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records. The Act serves two primary purposes:</p> <ol style="list-style-type: none"> 1. Gives parents and eligible students more control of their educational records 2. Prohibits educational institutions from disclosing “personally identifiable information for education records“ without written consent 	<ul style="list-style-type: none"> • Public or private school: elementary, secondary, post-secondary • State or local education agencies <p>Any of the above must receive funds under an applicable program of the U.S. Department of Education.</p>	<p>Student education record: Records that contain information directly related to a student maintained by an educational agency or institution or by a party acting for the agency or institution.</p>	<ul style="list-style-type: none"> • School officials • Schools to which a student is transferring • Specified officials for audit or evaluation purposes • Organizations conducting certain studies for or on behalf of the school • Appropriate officials in cases of health and safety emergencies • State and local authorities within a juvenile justice system, pursuant to specific state law • To comply with a judicial order or lawfully issued subpoena

<p>RCW 70.02 (General)</p> 	<p>The Uniform Health Care Information Act (UHCIA) provides confidentiality protection for medical records and patients’ health care information (HCI) and requires consent in most cases for release of records or disclosure of information, subject to certain exceptions.</p> <p>Washington law also contains provisions that are specific to the confidentiality of minors’ HCI, particularly with respect to parents’ access to that information.</p>	<p>Health care providers or persons who are licensed, certified, registered, or otherwise authorized by law to provide health care in the ordinary course of business or practice of a profession.</p> <p>There is a general assumption that entities beyond health care providers that handle a patient’s HCI are subject to this chapter.</p>	<p>HCI functions very similarly to PHI.</p> <p>HCI means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient’s health care.</p>	<ul style="list-style-type: none"> • To the individual • Treatment, payment, and health care operations • Research • Certain law enforcement purposes • In response to a serious threat to health and safety
<p>RCW 70.02.220 (STD info)</p> 	<p>Under Washington law, specific requirements govern confidentiality of information related to sexually transmitted diseases.</p>	<p>See RCW 70.02 (General)</p>	<p>“Information and records related to sexually transmitted diseases” means a type of health care information that relates to the identity of any person upon whom an HIV antibody test or other sexually transmitted infection test is performed, the results of such tests, and any information relating to diagnosis of or treatment for any confirmed sexually transmitted infections.</p>	<p>Disclosures without authorization are allowed under specific circumstances such as disclosures to:</p> <ul style="list-style-type: none"> • Legal representatives • Public health reporting and investigations • Claims management personnel for related payment purposes • Department of Children, Youth, and Families (DCYF), social workers, or legal guardians for placement purposes
<p>RCW 70.02.230 (Mental health info)</p> 	<p>Under Washington law, specific requirements govern confidentiality of information related to mental health services.</p>	<p>See RCW 70.02 (General)</p>	<p>“Information and records related to mental health services” means a type of health care information that relates to all information and records compiled, obtained, or maintained in the course of providing services by a mental health service agency or mental health professional to people who are receiving or have received services for mental illness.</p>	<p>Disclosures without authorization are allowed under specific circumstances such as disclosures to:</p> <ul style="list-style-type: none"> • Legal representatives • Courts or when required by law • Law enforcement when health and safety have been threatened • To or within Department of Social and Health Services, DCYF and HCA for treatment coordination purposes

Federal Confidentiality Laws

In 1996, Congress passed 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 significantly revised HIPAA when it passed the Health Information Technology for Economic and Clinical Health Act in response to the growth of distinct digital record formats and storage systems. More revisions have come since then.

Privacy Rule

The Privacy Rule provides federal protections for individually identifiable health information held by covered entities (defined later) and gives patients an array of rights with respect to that information. The Privacy Rule requires protected health information to be kept confidential and prohibits information from being shared without the valid consent of the patient who is the subject of the information, unless an exception applies.



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

Protected health information (45 CFR 160.103)

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.

PHI doesn't always have to directly identify an individual. You usually wouldn't know someone by their ProviderOne ID, for example. But if the information can be used to identify a person, even if it needs to be combined with other information for that to be possible, then it's PHI. Another

example of PHI is clinical notes, when they describe a person or their condition specifically (even if their name isn't present).

HIPAA-defined identifiers (45 CFR 164.514(b)(2)(i))

Many common identifiers are considered PHI, whether they directly identify the person or not. HHS has identified the following 18 identifiers as PHI:

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:
 - The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
 - The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people are 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 Uniform 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 in paragraph (c) in **HHS guidance**
18. Certificate/license numbers

It is important to be aware that, as item 17 states, this list includes nearly “any other unique identifying number, characteristic, or code,” so this list is not exhaustive. In short, if any number or characteristic identifies an individual, it should be considered PHI.

The above list is provided within the context of de-identifying data (45 CFR 164.514(b)(2)). Regardless of whether you intend to de-identify a dataset, the above list is intended to be a starting point for what is and is not PHI.

View the [HHS guidance on de-identification and these identifiers](#) 

Covered Entities (45 CFR 160.103)

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 (45 CFR 160.103)



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 include activities like claims processing, project management, professional services (e.g. legal, accounting, financial), and many others.

Some examples of business associates:

- A third-party administrator that assists a health plan with claims processing
- An attorney whose legal services to a health plan involve access to PHI
- An independent medical transcriptionist that provides transcription services to a physician
- A pharmacy benefits manager that manages a health plan’s pharmacist network

View the [HHS guidance on business associates](#) 

Business Associate Agreements (45 CFR 164.504(e)(1))

For an entity to become a business associate, they must execute a business associate agreement with the covered entity. In the business associate agreement, a covered entity must impose specified written safeguards on the PHI used or disclosed by the business associate. Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of PHI that would violate HIPAA.

View the [HHS guidance on business associate agreements](#) 

Minimum necessary standard (45 CFR 164.502(b))



The minimum necessary standard requires that PHI is only used or disclosed when it is necessary to satisfy a particular purpose, and that only the minimum amount be used necessary to accomplish the purpose.

As described below, a covered entity may disclose PHI only under certain circumstances. These disclosures are typically subject to the “minimum necessary standard.” If uncertain, assume the standard applies.

The minimum necessary standard does not apply to the following:

- Disclosures to 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 valid authorization
- Uses or disclosures that are required by other laws

Business associates must also abide by the minimum necessary standard.

View the [HHS guidance on the minimum necessary standard](#) 

Permitted uses and disclosures (45 CFR 164.502(a)(1))

The Privacy Rule generally prohibits a covered entity from using or disclosing PHI unless authorized by the patient. There are some circumstances where patient authorization is not required. HIPAA rarely requires disclosure of PHI.

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

- To the individual (unless the individual initiates the request, in which case it is required)
- 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
- Uses and disclosures where consent is not required
- 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.

View the [HHS guidance on individuals' right to access](#).

Treatment, Payment, and Health Care Operations

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.

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.

- **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.

View the [HHS guidance on disclosures for treatment, payment, and operations](#).

Incidental use and disclosure

The Privacy Rule does not require that every risk of 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.

View the [HHS guidance on incidental use and disclosure](#).

Authorization (45 CFR 164.508)

Unless specifically permitted or required by the Privacy Rule, a covered entity must obtain an individual's written authorization for any use or disclosure of PHI. The authorization must be written and include the following specific elements:

- A specific 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
- An expiration date or an expiration event that relates to the individual (e.g. "upon my death")
- Signed and dated by the individual or their authorized representative

A valid authorized must also include specific statements (see [45 CFR 164.508\(c\)\(2\)](#)). An example of a HIPAA-compliant authorization form is [HCA's standard form](#).

Uses and Disclosures Where Authorization is Required

Psychotherapy notes (45 CFR 164.508(a)(2))

With few exceptions, a covered entity must obtain a patient's authorization prior to a disclosure of psychotherapy notes **for any reason**, including regular disclosures for treatment, payment, and health care operations. The few exceptions

can be found in **45 CFR 164.508(a)(2)(i)**.

HHS has the position that psychotherapy notes are particularly sensitive information and that they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes.

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.”

More guidance from HHS on mental health information and psychotherapy notes is available on the HHS website and question and answer (Q&A) document.

 More guidance from HHS on mental health information and psychotherapy notes is available **on the HHS website** [↗](#) and **question and answer (Q&A) document** [↗](#).

Marketing (45 CFR 164.508(a)(3))

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.

View the **HHS guidance on marketing**.

Uses and Disclosures with Opportunity to Agree or Object (45 CFR 164.510)

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. These situations are most commonly found with providers treating patients. Some examples include maintaining facility directories, disclosures to an individual’s family members when they’re involved in the individual’s care, and in emergency circumstances when the disclosure is in the best interests of the individual.

View the **HHS guidance on these types of disclosures**.

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.

Required by Law

(45 CFR 164.512(a)) Covered entities may use and disclose PHI without individual authorization as required by law (including by statute, regulation, or court orders).

Public Health Activities

(45 CFR 164.512(b)) The Privacy Rule allows for disclosure without patient consent for certain public health activities. For example, a covered entity can 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 government authorities authorized to receive reports of child abuse and neglect.

View the **HHS guidance on disclosures for public health activities** [↗](#).

Victims of Abuse, Neglect or Domestic Violence

(45 CFR 164.512(c)) In certain circumstances, covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

Health Oversight Activities

(45 CFR 164.512(d)) Covered entities may disclose PHI to health oversight agencies (as defined in the Privacy 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.

Judicial and Administrative Proceedings

(45 CFR 164.512(e)) 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.

Law Enforcement Purposes

(45 CFR 164.512(f)) Covered entities may (but generally are not required to) disclose PHI to law enforcement officials for law enforcement purposes in certain circumstances. For example, a covered entity can disclose PHI to law enforcement officials to identify or locate a suspect, fugitive, material witness, or missing person.

View the [HHS guidance on PHI disclosures to law enforcement](#).

Research

(45 CFR 164.512(i)) 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.” When conducting research, researchers may obtain, create, use, and/or disclose PHI. The research must be reviewed and approved by an institutional review board.

View the [HHS guidance on disclosing PHI for research purposes](#) .

Serious Threat to Health or Safety

(45 CFR 164.512(j)) 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.

Notice of Privacy Practices (45 CFR 164.520)

Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contains certain elements. The notice must:

- Describe the ways in which the covered entity may use and disclose PHI
- State the covered entity’s duties to protect privacy, the covered entity’s privacy practices, and that the covered entity will abide by the terms of the current notice

- Describe individuals’ rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated
- 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. View the:

- [HHS guidance on notice of privacy practices](#)
- [HCA Apple Health \(Medicaid\) notice of privacy practices](#)
- [HCA Uniform Medical Plan \(UMP\) notice of privacy practices](#) for employee and retiree benefits, serving public and school employees

Individual Rights under HIPAA

Access

(45 CFR 164.524)

The HIPAA rules recognize the importance of individuals to be able to access and obtain a copy of their own health information. The Privacy Rule provides individuals with a legal, enforceable right to their PHI in a "designated record set" defined in 45 CFR 164.501.

View the [HHS guidance on individuals’ right to access](#).

Amendment

(45 CFR 164.526)

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

(45 CFR 164.528)

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

Restriction Request

(45 CFR 164.522)

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 people involved in the individual’s health care or payment for health care
- Disclosure to notify family members or others about the individual’s general condition, location, or death

Confidential Communication Requirements (45 CFR 164.522(b)(1))

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.

View the [HHS guidance on individual rights under HIPAA](#).

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

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 (45 CFR 164.308)

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.”

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

Physical Safeguards (45 CFR 164.310)

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 physical safeguard 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.

View the [HHS Guidance on physical safeguards](#).

Technical Safeguards (45 CFR 164.312)

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 enables it to 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.

View the [HHS guidance on technical safeguards](#).

Breach Notification Rule (45 CFR §§ 164.400-414)

The HIPAA Breach Notification Rule 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
- 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.

Notification Requirements

Note: State laws have notification requirements as well. See the section Breach notification under Washington State law.



Following a breach of unsecured PHI, covered entities must provide written 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.

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.

View the HHS guidance on the Breach Notification Rule [HHS HIPAA Breach Notification Rule](#).

Substance use disorder treatment

42 CFR Part 2

Certain SUD treatment information is subject to stringent regulations in 42 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, view HCA’s [Sharing Substance Use Disorder Information Guidance](#).

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. The primary source for confidentiality and the requirements for the release of HCI in Washington is found in the Uniform Health Care Information Act (UHCIA) 70.02 RCW, which Washington adopted in 1991.

UHCIA provides confidentiality protection for medical records and patients' HCI and requires consent in most cases for the 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 run parallel with the federal HIPAA Privacy Rule, but state law includes 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 UHCIA, the term "health care information" means any information, whether oral or recorded in any form or medium, that meets all three of the following requirements:

- It is created or received by HCA concerning a client or potential client.
- It 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.
- It 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 UHCIA.

Allowable uses and 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 from the individual or their personal representative.

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 UHCIA 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 18 to voluntary termination of pregnancy as long as the fetus is not viable
- A minor parent with sufficient capacity may consent to medical treatment for their child
- An unaccompanied homeless youth for nonemergency, outpatient, or outpatient services (RCW 7.70.065(3))

Accordingly, a minor may authorize the release of HCI in the above situations if 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 (statement) of a parent that the parent is authorized to consent to health care on behalf of the minor patient, regardless of whether:

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

Washington minor consent laws

When a parent or guardian's consent is required.

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 an Unaccompanied Homeless Youth, emancipated, or married	Smith v. Seibly, 72 Wn. 2d 16 (1967) RCW 7.70.065(3)
Immunizations	Yes, unless minor is an Unaccompanied Homeless Youth, emancipated, or married	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 treatment, without parental consent.
Inpatient substance abuse treatment	Yes, unless the 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 treatment without parental consent if DSHS determined child is in need of services.

When a minor can consent based on legal status.

Status	Minor Consent	Notes	Citations
Age of majority	Younger than 18: no Age 18 and above: yes	Age of majority is 18	RCW 26.28.010; 26.28.015
Emancipated minor	Yes	Emancipated minor may consent	RCW 13.64.060
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
Unaccompanied Homeless Youth	Yes	Authorized for nonemergency, outpatient, primary care services	RCW 7.70.065(3)

Authorization Elements

The essential elements to a valid authorization under Washington law are the same as a HIPAA-compliant authorization (see the section Authorization, 45 CFR 164.508).

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.

STDs: permitted and mandatory disclosures

(RCW 70.02.220) No entity may disclose or be compelled to disclose information and records related to STDs unless specifically authorized by law. An entity may disclose HCI related to an individual's STDs pursuant to a valid authorization, or without authorization only in certain circumstances. Refer to the regulation for the [full list of permitted disclosures](#).

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 without authorization only in certain circumstances. Refer to the regulation for the [full list of permitted disclosures](#).

Breach notification under Washington State law (RCW 42.56.590 and 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 if it has determined that a breach of personal information has occurred.

Notification obligation

Much like HIPAA, an entity must notify all affected Washington residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice is not required if the breach is not reasonably likely to harm the affected individual, or if the improperly disclosed HCI was secured or otherwise rendered unreadable.

Attorney general notification

An entity that suffers a breach affecting more than 500 Washington residents must submit a sample copy of the notification letter (excluding any personally identifiable information) to the Washington State Attorney General. the information identified above is unknown at the time the notice is due.

Timing of Notification

The notification to affected individuals and to the Attorney General (if applicable) must be made within 30 calendar days after the breach was discovered.

A delay beyond this deadline may be permitted if it is at the request of law enforcement, or if the delay is necessary to determine the scope of the breach and to restore integrity of affected data systems.

When also subject to HIPAA

Covered entities (as defined by HIPAA) are deemed to have complied with these state requirements 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 (RCW 42.56.592 and 19.255.030).

Use of electronic signatures (RCW 1.80.040)

RCW 1.80 permits the use of electronic signatures with the same force and effect as a handwritten signature. A signature in any form must be attributed to the person based on the context and surrounding circumstances at the time of the signature.

View the [HCA guidance on valid electronic signatures](#).

2024 Updates to reproductive health privacy

HIPAA Privacy Rule to Support Reproductive Health Care Privacy

On April 22, 2024, the Biden-Harris Administration issued a new **HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy** (Final Rule) which provides heightened protections for PHI relating to reproductive care in certain circumstances. The Final Rule was issued in response to the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, which overturned long standing protections from *Roe v. Wade*. requested to investigate any person in connection with seeking, obtaining, providing, or facilitating reproductive healthcare that is lawful under the circumstances in which it is provided.

Prohibition

The Final Rule prohibits the use or disclosure of PHI for any of the following activities:

- To conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided.
- The identification of any person for the purpose of conducting such an investigation or imposing such liability.

Attestation

In some circumstances, when a covered entity receives a request for PHI potentially related to reproductive health care, it must obtain a signed attestation from the requester that the use or disclosure is not for a purpose prohibited by the Final Rule. This attestation requirement applies in the following circumstances:

- Health oversight activities.
- Judicial and administrative proceedings.
- Law enforcement purposes.
- Disclosures to coroners and medical examiners.

View the [HHS guidance on all requirements of the Final Rule](#).

Washington My Health My Data Act (RCW 19.73)

The My Health My Data Act is the first privacy-focused law in the country to protect personal health data falling outside HIPAA's jurisdiction. While HIPAA applies to entities like health care providers and health plans, this law applies to businesses. The act was developed to protect an individual's sensitive health data from being collected and shared without that individual's consent.

The act applies to data "collected" (broadly defined) in Washington, regardless of the individual's state or residency. The act also applies to a broad range of data categories including location that may reveal someone's access to healthcare services, even where such data is not specifically tied to health characteristics or processed by HIPAA covered entities.

Under the My Health My Data Act, individual health data is defined as "personal information that is linked or reasonably linkable to an individual and that identifies the individual's past, present or future physical or mental health status." Please see [examples listed in this regulation](#).

View the [guidance on the My Health My Data Act](#) on the Washington State Attorney General's Office website.