# Privacy

The purpose of this section is to address the importance of safeguarding client’s information, which includes client protected health information (PHI), to:

* Protect the privacy rights of clients when DSHS uses, obtains, maintains, or

discloses client confidential information;

* Ensure responsible information governance and management practices;
* Promote public trust and confidence in the use of services provided by the DSHS;

and

* Maintain the confidentiality, integrity, and availability of PHI and other confidential information, while protecting against any reasonably anticipated threats, hazards, and inappropriate uses or disclosures.

**What is Privacy?**

The right of a person to be free from intrusion into or publicity concerning matters of a personal nature. *(Merriman Webster Legal Dictionary)*

#### Ask the Expert

If you have questions or need clarification about the content in this chapter, please contact:

Cynthia Mitchell HCS Division Privacy Program Manager

 360.725.2537 office

 cynthia.mitchell@dshs.wa.gov

## Table of Contents

Privacy: 1

What is Privacy?............................................................................................................................................1

Ask the Expert: 1

Background: 3

DSHS Privacy Policies:………………………………………………………………………………………………………………………………3

Definitions and Examples:…………………………………………………………………………………………………………………….3-5

All Client Information is Confidential:………………………………………………………………………………………………………5

Where Privacy Applies:……… ……………….………………………………………………………………………………………………….5

Common Causes in Reported Incidents:..…………………………………………………………………………………………………5

Other Poor Practices:………………………………………………………………………………………………………………………………6

Best Practices for Protecting Confidential Information:.………………………………………………………………………….6

HIPAA Basics:………………………………………………………………………………………………………………………………………..…6

HIPAA Basics - Exclusions:……………………………………………………………………………………………………………………….7

Overview of HIPAA:………………………………………………………………………………………………………………………………..7

Special Consideration for Mailing:.....……………………………………………………………………………………………………..7

Standard: De-Identification of Protected Health Information:..………………………………………………………………7

Procedures for Managing a Privacy Breach:..………………………………………………………………………………………….8

Step 1: Reporting the Breach:..………………………………………………………………………………………………………….……8

Step 2: Containing the Breach:………………………………………………………………………………………………………………..8

……………………………..(Privacy Breach Questionnaire & Internal Lost-Stolen Data Checklist):…………………….8

Step 3: Evaluating the Risks Associated with the Breach:……………………………………………………………………..8-9

……………………………...(Department's (HCC's) Health Care Components:..………………………………………………....9

……………………………...(Mitigation Actions & Examples):…………………………………………………………………….…9-10

Step 4: Notification:……………………………………………………………………………………………………………………………….10

………………………………(When to Notify)…………………………………………………………………………………….....………….10

……………………………….(How to Notify):…………………………………………………………………………………………….…..…10

……………………………….(Substitute Service):……………………………………………………………………………………………..10

……………………………….(What to Include):……………….………………………………………………………………………..…10-11

Attorney General and Federal Trade Commission Websites:..……………………………………………………………….11

Three Major Credit Report Agencies:…………………………………………………………………………………………….………11

Others to Notify:..………………………………………………………………………………………………………………………….…11-12

Destruction or Return Requirement:…………………………………………………………………………………………………....12

Corrective and Disciplinary Actions for Breaches:..…..…………………………………………………………………………..12

For More Information:..……………………………………………………………………………………………………………….……….13

Resources:.…………………………………………………………………………………………………………………………………………..13

Related RCWs and CFRs:......………………………………………………………………………………………………………………...13

Related Administrative Policies..…………………………………………………………………………………………………………..13

Related Links and Websites:………………………………………………………………………………………………………………….13

Sample Letters and Forms:……………………………………………………………………………………………………………..……..13

Contacts:.....................................................................................................................................................14

Acronyms:……………………………………………………………………………………………………………………………………………..14

## Background

Employees who work at the Department work daily with many confidential records and must act to protect those records and the privacy rights of individuals. The Department is a Hybrid Covered Entity under the HIPAA Privacy Rule, which requires safeguards for client information and the reporting of any breach of security of client information. As a covered entity, DSHS must notify affected clients of Health Information Portability and Accountability Act (HIPAA) privacy rights. (45 CFR 164.520) DSHS programs that are designated as Health Care Components or HCCs are part of the Hybrid Covered Entity.

The obligations of Department employees are set out in DSHS [Administrative Policy 5.01](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?xsdata=MDV8MDJ8fGYzYmE1MjAwMWU2MzQ2YWQ0MTY3MDhkYzRmNWRmMjdkfDExZDBlMjE3MjY0ZTQwMGE4YmEwNTdkY2MxMjdkNzJkfDB8MHw2Mzg0NzI1MTIwOTg2MTU2NTV8VW5rbm93bnxWR1ZoYlhOVFpXTjFjbWwwZVZObGNuWnBZMlY4ZXlKV0lqb2lNQzR3TGpBd01EQWlMQ0pRSWpvaVYybHVNeklpTENKQlRpSTZJazkwYUdWeUlpd2lWMVFpT2pFeGZRPT18MXxMMk5vWVhSekx6RTVPakZoTVdFeU16Z3hMV1JrWTJFdE5EVTJOQzFoWVRnd0xXVmtOamd4TXpJMU1ERmlPRjgyWldVek5HTXlPQzFtTmpNekxUUTVOV1V0WWpkbE1TMDNOV0UzTm1JMU1tVmxNVEJBZFc1eExtZGliQzV6Y0dGalpYTXZiV1Z6YzJGblpYTXZNVGN4TVRZMU5EUXdPVFUyTUE9PXxjYzJkOThhZTBlZWU0MmIyZGYzNTA4ZGM0ZjVkZjI3YXwwNzYwZTAzMWVkNzk0N2E3ODJkYjBkZTZmMzE5ODk0MQ%3D%3D&sdata=ZS9RcjU2QVh6MnptVnFsRmt3Nm9TN1ZXODJFR3RxOUpmekRVOW4zdksybz0%3D&ovuser=11d0e217%2D264e%2D400a%2D8ba0%2D57dcc127d72d%2Ccynthia%2Emitchell%40dshs%2Ewa%2Egov&OR=Teams%2DHL&CT=1711723292349&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiIyNy8yNDAyMDExOTMwNyIsIkhhc0ZlZGVyYXRlZFVzZXIiOmZhbHNlfQ%3D%3D&id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D05%2D01%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) and the [IT Security Policy 15.10](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D15%2D10%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative). The rights of clients are described in [DSHS Administrative Policy 5.03](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D05%2D03%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative)

Employees must follow DSHS policies and procedures in the [DSHS information security manuals](https://stateofwa.sharepoint.com/sites/DSHS-EXE-IT-Standards/SitePages/DSHS-Information-Security-Standards-Manual.aspx) for accessing, handling, and disclosing confidential information. In addition, employees of HCCs (including BAOUs) must follow the HIPAA rules for use or disclosure of PHI.

**DSHS Privacy Policies**

Administrative Policy 5.01- Privacy Policy

*Establishes Privacy Officer and Coordinators; HIPAA Hybrid; General Requirements to protect Confidential Information.*

Administrative Policy 5.03- Client Rights

 *Client Rights to Protected Health Information*

*Administrative Policy 5.08- DSHS Minimum Physical Security Standards*

**definitions and examples**

**Breach:** The acquisition, access, Use, Disclosure, or loss of Confidential Information in a manner not permitted by state and federal law that compromises the security, privacy, or integrity of the Confidential Information.

**Breach Notification Rule:** Requires covered entities and Business Associates (contractors) to provide notification following discovery of a breach of unsecured Protected Health Information (PHI; and the enforcement rule which provides authority and procedures for OCR investigations, imposition of penalties, and administrative hearings.

**Business associate:** A person who, on behalf of DSHS other than in the capacity of a member of

the workforce, performs a function or activity involving the use or disclosure of protected

health information (PHI) to carry out essential functions or perform services for DSHS.

“Business associates” include subcontractors that create, receive, maintain or transmit PHI on

behalf of the business associate and downstream contractors.

**Client:** A person who receives services or benefits from DSHS. This term includes, but is not

limited to, consumers, recipients, applicants, residents of DSHS facilities or institutions,

patients, and parents receiving support enforcement services. Clients include persons who

previously received services or benefits and persons applying for benefits or services.

 **Client confidential information:** Personally Identifiable Information, including PHI, which

identifies a client, and that state or federal laws protect from improper disclosure or use.

**Covered entity:** A covered entity is a health plan, a health care clearinghouse, or a health care

provider who transmits information electronically in connection with a HIPAA transaction (see

45 CFR 160.103). As defined in 45 CFR 164.103, DSHS is a hybrid entity that has designated programs as health care components within the administrations/divisions as provided on the DSHS website. As a hybrid entity, only its health care components (including BAOUs) are subject to the HIPAA rules**. See BAOUs definition in AP 5.01.**

**HIPAA:** The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq. To implement HIPAA, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) has adopted the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule (See 45 CFR Parts 160 and 164).

**HIPAA Rules:** References to the “HIPAA rules” apply to the following rules that OCR enforces;

* **The HIPAA Privacy Rule:** protects the privacy of individually identifiable health

information;

* **The HIPAA Security Rule:** sets national standards for the security of electronic

protected health information;

* **The HIPAA Breach Notification Rule**: requires covered entities and business associates to provide notification following a breach of unsecured PHI; and the enforcement rule which provides authority and procedures for OCR investigations, imposition of penalties, and administrative hearings.

**Hybrid entity: A single legal entity:**

1. That is a covered entity;

2. Whose business activities include both covered and non-covered functions; and

3. That designates health care components in accordance with the HIPAA privacy rule.

DSHS is a hybrid entity under the HIPAA privacy rule.

**Individually identifiable**: Means that a record contains information, which reveals or can likely

be associated with the identity of the person or persons to whom the record pertains.

**Examples:**

* Names, addresses, client ID numbers, and unique characteristics. Also, may be known as

*individually identifiable health information or “IIHI*”.

**Minimum necessary**: The minimum amount of protected health information (PHI) needed to

accomplish the purpose of a request for PHI or the use of PHI needed to perform one’s job.

* The Privacy Rule requires that DSHS make reasonable efforts to ***limit the use of PHI to the minimum necessary*** for the intended purpose.

**Protected health information (PHI):** Individually identifiable health information about a client

that is transmitted or maintained by a DSHS health care component in any form or medium.

PHI includes demographic information that identifies the individual or about which there is

reasonable basis to believe can be used to identify the individual. Individually identifiable health information in DSHS records about an employee or others who are not clients is not protected health information. See administrative policy 5.03 for provisions relating only to PHI of clients.

**Use:** Access to and application or analysis of confidential information within DSHS.

**Willful neglect:** The conscious, intentional failure or reckless indifference to the obligation to

comply with the HIPAA rules. (See 45 CFR 160.401).

**All Client Information is Confidential**

All information about clients served on behalf of DSHS is confidential, including:

* + The fact that they get assistance (except yes/no)
	+ Type of assistance or services received
	+ Demographic information of clients (name, address, SSN, client ID#, photos)

**Where Privacy applies:**

* Information Technology - Creation, Transmission, Storage
* Maintaining and Storing Records
* Configuration and Access to Physical Spaces
* Interactions with Clients – In Person, Phone, Mail, Email

**Common causes in reported incidents**

* Wrong Email Address (Autofill!!!!)
* Wrong Fax Number
* Excel Sheet errors
* Theft from car

**Other poor practices**

* Leaving Devices Unsecure and Unattended
* Using Unsecure Channels of Communication
* Disposing of PHI Improperly
* Accessing PHI Out of Curiosity
* Sharing PHI on Social Media
* Discussing confidential information in a public area or in an area where the public could overhear the conversation.

**Best Practices for Protecting Confidential Information**

* + Encrypt electronic devices
	+ Do not leave client information in a vehicle unattended
	+ Check email addresses before sending an email (or fax numbers when faxing)
	+ Check that envelopes are stuffed and addressed properly
	+ Do not download or store confidential records on your home computer
	+ Do not share client information with unauthorized third parties – (e.g. media, union representative, etc.)
	+ Do not send client-related emails to your personal email account or outside the network
	+ Properly dispose of confidential records (hot trash)
	+ Don’t use identifiable information when others can overhear or if not needed

**HIPAA Basics**

Health Insurance Portability and Accountability Act of 1996 Required rules for privacy , national standards for electronic health care transactions.

Privacy Rule (2002) – regulates the circumstances under which covered entities may use and disclose Protected Health information and requires covered entities to have safeguards in place to protect the privacy of the information.

Security Rule (2003) – requires covered entities to implement certain administrative, physical, and technical safeguards to protect electronic information.

Breach Notification Rule (2009) – requires covered entities and Business Associates to provide notification following discovery of a breach of unsecured protected health information.

Rules implementing HIPAA are in 45 CFR parts [160](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160?toc=1) and [164](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164?toc=1). All rules apply to Business Associates of covered entities and their subcontractors

**HIPAA Basics – Exclusions**

HIPAA does not apply to anyone who is not a covered entity or covered entity’s

business associate.

Information that is not protected health information:

• Education records covered by Family Educational Rights and Privacy Act

(FERPA) or students’ health records

• Employment records held by DSHS in its role as employer (i.e. workforce

members)

• Records of persons deceased more than 50 years

 **Overview of HIPAA**

* Privacy Rule – Keep PHI private
* Security Rule – Keep PHI secure
* Breach Notification Rule – If you don’t keep PHI private and secure, you have to notify!

PHI = Protected Health Information (defined term under HIPAA)

**SPECIAL CONSIDERATIONS FOR MAILING**

* + Use of First-Class mail or delivery services with tracking
	+ Carefully check the name and address of the intended recipient
	+ Check the contents before sealing and make sure there is nothing included that is intended for a different client
	+ Update names and addresses when notified of correction or change
	+ Report as potential breach if mailing sent to unintended recipient

**Standard: De-identification OF PROTECTED HEALTH INFORMATION**

1) Names 6) Medical record numbers

2) Telephone numbers 7) Health plan beneficiary numbers

3) Fax numbers 8) Account numbers

4) Electronic mail addresses 9) Certificate/license #s

5) Social security numbers 10) Device identifiers & serial #s

 11) Web Universal Resource Locators (URLs)

 12) Internet Protocol (IP) address #s

 13) Vehicle identifiers and serial numbers, including license plate numbers

 14) Biometric identifiers, including finger and voice prints

 15) Full face photographic images and any comparable images

 16) Any other unique identifying #, characteristic, or code (e.g. client ID)

 17) All geographic subdivisions smaller than a State

 18) All elements of dates (except year) for dates directly related to an individual,

 including birth date, admission date, discharge date, date of death

**PROCEDURE FOR MANAGING A PRIVACY BREACH**

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure, or disposal of Client PHI. All incidents are presumed a breach unless proven otherwise. An example of a privacy breach would be lost, stolen, or personal information mistakenly emailed to the wrong person.

**Step 1: reporting the breach**

If a Breach or potential Breach of Confidential Information is discovered, staff at a minimum must notify within one (1) business day of discovery:

1. The technology operations center (TOC) at ETOC@dshs.wa.gov; and
2. The administration’s or division’s Privacy Coordinator. (Please see [DSHS Privacy Coordinators](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OIG-Privacy).)
3. For Breaches involving over 500 individuals, or potentially over 500 individuals, staff must also notify the DSHS Privacy Officer at DSHSprivacyofficer@dshs.wa.gov. The DSHS Privacy Officer may also be consulted on other Breaches as appropriate and necessary.

**Step 2: containing the breach**

It is necessary to immediately contain the breach. Some examples of containing a breach are:

* Ensuring a police report has been filed if the breach involved criminal activity;
* recovering records;
* and confirming deletion of emails sent to wrong persons.

**Privacy Breach Questionnaire**: The Privacy Breach Questionnaire must be completed.

Once information is provided to us, we can determine the nature of the notification needed to ensure the breach is fully disclosed to clients affected, and whether or not additional steps are necessary to protect clients from identity theft or unwanted intrusion into their personal information.

 **Privacy Breach Questionnaire can be found** [**here**](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Privacy%20Breach%20Questionnaire.docx)**.**

 **Internal Lost-Stolen Data Checklist can be found** [**here**](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Internal%20Lost-Stolen%20Data%20Checklist.docx)**.**

**Step 3: Evaluating the risks associated with the breach**

The Risk Assessment is vital and required by HIPAA. The designated Privacy Coordinator must complete the HIPAA breach risk assessment in the DSHS Privacy Breach Application (PBA) for incidents that are determined to be a HIPAA Breach along with the DSHS security breach report. The DSHS security breach report is available for completion in the privacy breach application once an incident is determined to be a breach.

**The following factors will be among those considered when assessing the risks.**

1. **Persons affected by the breach**
	1. How many clients are affected by the breach?
2. **Protected Health Information Involved**
	1. What data elements have been breached?
* Name, social security number, date of birth, and financial information that could be used for identity theft are examples of PHI.
1. **Description and Extent of Breach:**
	1. What caused the breach?
	2. Was the information PHI?
	3. Is there a risk of ongoing or further exposure of the information?
	4. Was the information secured? Meaning was it encrypted or otherwise unusable, unreadable, or indecipherable to unauthorized individuals?
	5. Does the confidential information involve records of clients held by a program that is a HCC of the Department or a business associate (inside or outside of DSHS) of a HCC component as listed in DSHS hybrid entity designation?

**For a list of the Department’s HCCs click** [**here**](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OIG-Privacy/Components/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOIG%2DPrivacy%2FComponents%2F03%2D387B%20Health%20Care%20Components%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOIG%2DPrivacy%2FComponents)**.**

1. **Four Part Test**: (The HIPAA breach risk assessment applies the four-part test required by HIPAA to adequately document the determination that the incident is not a Breach).
* **Part 1:** Nature and extent of PHI involved, including types of identifiers and ability to identify individual.
* **Part 2:** Nature of person who acquired, accessed, used or received the PHI:
* **Part 3:** Risk whether PHI was actually accessed or acquired by unauthorized individual:
* **Part 4:** Mitigation Actions taken as a result of the breach: **(Steps taken to ensure that the incident won’t happen again).**

 Mitigation is required by HIPAA under 45 CFR 164.530(f). To the extent practicable, DSHS and its employees must mitigate any harmful effect known to the agency of a breach or a use or disclosure of PHI that violates DSHS policies and procedures and the HIPAA Rules. Mitigation actions must be documented and provided to the DSHS privacy officer upon request.

 **Examples of Mitigation Actions**:

* Verbally counseled responsible employee on HIPAA and administrative policies for managing the protection of PHI.
* Completed LC- HIPAA Mandatory Training
* Reviewed DSHS Information Security Standard Manual: Chapters 3, 7, 8

**Step 4: NOTIFICATION**

If notification is required as a result of a breach of confidential information, employees must contact their administration or division privacy coordinator. Breach notice letters must contain any specific language that the applicable law requires and be sent within the required time. Any notification letters required by HIPAA or RCW 42.56.590 must be reviewed and approved by the program’s designated privacy coordinator, or the DSHS privacy officer or designee.

For breach incidents that do not trigger a legal requirement for notification, it is up to the program to determine to notify. However, DSHS strongly encourages notification.

1. **When to Notify Affected Individuals**
* Notification to affected individuals must be made in the most expedient time possible, without unreasonable delay, and no more than thirty (30) calendar days after the breach was discovered. An agency may delay notification to the consumer for up to an additional fourteen (14) days to allow for notification to be translated into the primary language of the affected consumers.
1. **How to Notify Affected Individuals**
	1. Written notice. (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
	2. Under HIPAA, a deceased person's Protected Health Information (PHI) is protected for 50 years from death. If the affected individual is known to be deceased, the covered entity must send notification via first-class mail to either the next of kin or personal representative of the individual.
2. **Substitute Service**
3. 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.
4. **What must be Included in the Notification**

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting agency;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

**Attorney General and Federal Trade Commission Websites**

If affected individuals are concerned about their identity or credit being impacted, they can find information on actions to take to protect themselves on the websites of the Washington State Office of the Attorney General at: <http://www.atg.wa.gov/identity-theftprivacy> and for the Federal Trade Commission at: <http://www.ftc.gov/bcp/edu/microsites/idtheft//>.

**Three major credit report agencies**

In addition, the affected individuals can contact the three major credit report agencies:

* *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](https://www.equifax.com/), 1-800-685-1111
* *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](https://www.experian.com/), 1-888-397-3742
* *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](https://www.transunion.com/), 1-800-916-8800

**Others to Notify**

1. NOTICE TO THE SECRETARY
2. If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.
3. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.
4. MEDIA
5. If a breach affects more than 500 individuals, the covered entity is required to notify prominent media outlets serving the state or jurisdiction.
* This is typically done in the form of a press release to local media outlets servicing the affected area. Similar to individual notices and notices to the secretary, media notification must be provided without unreasonable delay and in no case later than 60 days following discovery of the breach must include the same information required for the individual notice.
1. AP Policy 2.07 requires press releases to go through the DSHS Office of Communications.
2. STATE ATTORNEY GENERAL OFFICE (AGO) (RCW 42.56.590)
* Under 42.56.590(7) for any breach over 500, a covered entity must also notify the AGO no more than thirty days after the breach was discovered.

(a) The notice to the attorney general must include the following information:

(i) The number of Washington residents affected by the breach, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;

(iv) A summary of steps taken to contain the breach; and

(v) A single sample copy of the security breach notification, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

**Destruction or Return Requirement:**

If you receive healthcare information that you are not authorized to receive, *contact the sender* *to notify so they are aware you have received the information in error,* and then destroy the information without further dissemination.

* You may also follow the sender’s instruction on how to return the health care information to the entity *and confirm no further dissemination*.

**Corrective and disciplinary action for violations**

* Employees found to be in violation of DSHS policies and procedures relating to confidentiality of PHI or other Confidential Information may receive corrective or disciplinary action, up to and including dismissal. Training and other mitigation steps may also be required as a result of Breaches or violations of confidentiality laws. DSHS and its employees are subject to civil and criminal fines and sanctions by the Department of Health and Human Services – Office for Civil Rights for violations of the HIPAA Rules. Civil penalties for violations of HIPAA Rules may be imposed up to $50,000 per violation for a total of up to $1,500,000 for violations of each requirement during a calendar year. Criminal penalties may total up to $250,000- and ten-years imprisonment.

**For more information**

If you are unsure about appropriate use or disclosure of PHI, or if you need more information about your obligations to protect the privacy of information, consult the following resources:

* Your employer’s administrative and IT security policies
* Your employer’s Privacy Officer
* 45 CFR Parts [160](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160?toc=1) and [164](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164?toc=1) (The Privacy Rule, which establishes federal protection for the privacy of health information.

**Resources**

**Related RCWs and CFRs**

[RCW 42.56.590](http://app.leg.wa.gov/RCW/default.aspx?cite=42.56.590) Personal information—Notice of security breaches

[45 CFR 164.520](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/privacy-practices-for-protected-health-information/index.html) Notice of Privacy Practices for Protected Health Information

45 CFR 160 General Requirements

45 CFR 164 Security and Privacy

**Related Administrative Policies**

[Administrative Policy 5.01](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?xsdata=MDV8MDJ8fGYzYmE1MjAwMWU2MzQ2YWQ0MTY3MDhkYzRmNWRmMjdkfDExZDBlMjE3MjY0ZTQwMGE4YmEwNTdkY2MxMjdkNzJkfDB8MHw2Mzg0NzI1MTIwOTg2MTU2NTV8VW5rbm93bnxWR1ZoYlhOVFpXTjFjbWwwZVZObGNuWnBZMlY4ZXlKV0lqb2lNQzR3TGpBd01EQWlMQ0pRSWpvaVYybHVNeklpTENKQlRpSTZJazkwYUdWeUlpd2lWMVFpT2pFeGZRPT18MXxMMk5vWVhSekx6RTVPakZoTVdFeU16Z3hMV1JrWTJFdE5EVTJOQzFoWVRnd0xXVmtOamd4TXpJMU1ERmlPRjgyWldVek5HTXlPQzFtTmpNekxUUTVOV1V0WWpkbE1TMDNOV0UzTm1JMU1tVmxNVEJBZFc1eExtZGliQzV6Y0dGalpYTXZiV1Z6YzJGblpYTXZNVGN4TVRZMU5EUXdPVFUyTUE9PXxjYzJkOThhZTBlZWU0MmIyZGYzNTA4ZGM0ZjVkZjI3YXwwNzYwZTAzMWVkNzk0N2E3ODJkYjBkZTZmMzE5ODk0MQ%3D%3D&sdata=ZS9RcjU2QVh6MnptVnFsRmt3Nm9TN1ZXODJFR3RxOUpmekRVOW4zdksybz0%3D&ovuser=11d0e217%2D264e%2D400a%2D8ba0%2D57dcc127d72d%2Ccynthia%2Emitchell%40dshs%2Ewa%2Egov&OR=Teams%2DHL&CT=1711723292349&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiIyNy8yNDAyMDExOTMwNyIsIkhhc0ZlZGVyYXRlZFVzZXIiOmZhbHNlfQ%3D%3D&id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D05%2D01%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) Privacy Policy -- Safeguarding Confidential Information
[Administrative Policy 5.03](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D05%2D03%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) Client Rights Relating to Protected Health Information

[IT Security Policy 15.10](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D15%2D10%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) Information and Technology Security

[DSHS information security manuals](https://stateofwa.sharepoint.com/sites/DSHS-EXE-IT-Standards/SitePages/DSHS-Information-Security-Standards-Manual.aspx) DSHS Information Security Manual

[Administrative Policy 2.07](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D02%2D07%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) Visual Communications Policy

[Administrative Policy 5.08](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OJCR/Administrative/Forms/AllItems.aspx?id=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative%2FDSHS%2DAP%2D05%2D08%2Epdf&parent=%2Fsites%2FDSHS%2DEXE%2DOJCR%2FAdministrative) DSHS Minimum Physical Security Standards

**Related Links and Websites**

[HIPAA Breach Notification Rule](https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)  HIPAA Breach Notification Rule

[HIPAA Covered Programs (HCC List)](https://forms.dshs.wa.lcl/formDetails.aspx?ID=80792) Department’s HCC List

<http://www.atg.wa.gov/identity-theftprivacy> WA State Office of the Attorney General

<http://www.ftc.gov/bcp/edu/microsites/idtheft//> The Federal Trade Commission

[www.equifax.com](https://www.equifax.com/%22%20%5Ct%20%22_blank) Equifax

[www.experian.com](https://www.experian.com/) Experian

[www.transunion.com](https://www.transunion.com/) TransUnion

**Sample Letters and Forms**

[Sample RCW 42-56-590 Client Notification Letter](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Sample%20RCW%2042-56-590%20Client%20Notification%20Letter.doc)

[Sample HIPAA breach notification letter by HCC](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Sample%20HIPAA%20breach%20notification%20letter%20by%20HCC.doc)

[Privacy Breach Questionnaire](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Privacy%20Breach%20Questionnaire.docx)

[Internal Lost-Stolen Data Checklist](https://stateofwa-my.sharepoint.com/personal/cynthia_mitchell_dshs_wa_gov/Documents/LTC%20Chapter%20Info/3-2025/Internal%20Lost-Stolen%20Data%20Checklist.docx)

**Contacts**

DSHSprivacyofficer@dshs.wa.gov The DSHS Privacy Officer

ETOC@dshs.wa.gov The technology operations center (TOC

[DSHS Privacy Coordinators](https://stateofwa.sharepoint.com/sites/DSHS-EXE-OIG-Privacy) DSHS Privacy Coordinators

**Acronyms**
AGO Attorney General Office

AP Administrative Policy

BAOU Business Associate Organizational Units

FERPA Family Educational Rights and Privacy Act

HCC Health Care Component

HIPAA Health Information Portability and Accountability Act
IP Internet Protocol

OCR Office for Civil Rights

PBA Privacy Breach Application

PHI Protected Health Information

TOC Technology Operations Center

URL Universal Resource Locators

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Made By** | **Change(s)** | **MB #** |
| 4/30/2025 | Cynthia Mitchell | Updated the Purpose, added Privacy definitionAdded DSHS Privacy PoliciesAdded more info about breach notification ruleRemoved unsecure phi infoAdded Business Associate definitionAdded Client definitionAdded Client Confidential Information definitionUpdated definition of Covered EntityUpdated HIPAA RulesAdded Individually identifiable:Updated Hybridization Updated Min Necessary definition Added PHI definitionAdded Use definitionAdded Willful neglect definitionAdded Where Privacy AppliesAdded Common Causes in Reported IncidentsAdded HIPAA BasicsRemoved – when HIPAA does not apply AND added HIPAA Basics – and ExclusionsAdded Overview of HIPAAAdded Requirements of Mitigation to Part 4Updated Step 4: Notification informationUpdated when to Notify affected indivUpdated how to notify affect indivUpdated substitute serviceUpdated what must be Included in the NotificationUpdated Three major credit report agenciesChanged Consequences for Breaches to - Corrective and disciplinary action for violationsUpdated definition to 45 CFR Parts 160 and 164Updated cfr’sUpdated links/websitesUpdated 42.56.590 client notification letterUpdated contracts and acronyms |  |