# Privacy

The purpose of this section is to address the importance of handling and protecting client health information to ensure privacy and confidentiality, and the steps to take once a breach has occurred.

Table of Contents

[**Privacy: 1**](#_Toc536776244)

[Ask the Expert: 2](#_Toc536776245)

[Introduction: 2](#_Toc536776246)

Definitions and Examples:…………………………………………………………………………………………………………………..2

All Client Information is Confidential:………………………………………………………………………………………………….3

Best Practices for Protecting Confidential Information:.………………………………………………………………………4

When HIPAA Does Not Apply:……………………………………………………………………………………………………………..4

Special Consideration for Mailing:.....………………………………………………………………………………………………….4

De-Identification Standards for HIPAA/HICA:.……………………………………………………………………………………..4

[Procedures](#_Toc536776251) for Managing a Privacy Breach:..……………………………………………………………………………………… 5

[Step](#_Toc536776252)1: Reporting the Breach:..**……………………………………………………………………………………………………. 5**

[Step 2: Containing the Breach: **5**](#_Toc536776253)

[Step 3: Evaluating the Risks Associated with the Breach: **6**](#_Toc536776254)

Step 4: Notification:[**……………………………………………………………………………………………………………………..7**](#_Toc536776255)

**Attorney General and Federal Trade Commission Websites:..……………………………………………………………..8**

**Three Major Credit Report Agencies:…………………………………………………………………………………………………..8**

**Others to Notify:..…………………………………………………………………………………………………………………………….…9**

**Destruction or Return Requirement: 9**

**Consequences for Breaches:..…..…………………………………………………………………………………………….…………. 9**

**For More Information:..……………………………………………………………………………………………………………….……10**

**Resources:.……………………………………………………………………………………………………………………………………….10**

[Related](#_Toc536776263) RCWs and CFRs:**......……………………………………………………………………………………………………….10**

Related Administrative Policies..**…………………………………………………………………………………………………10**

Related Links and [Websites:**……………………………………………………………………………………………………….10**](#_Toc536776264)

Sample Letters and Forms:………………………………………………………………………………………………………………..10

Contacts:............................................................................................................................................10

[Acronyms:](#_Toc536776266)…………………………………………………………………………………………………………………………………………11

## Ask the Expert

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

Cynthia Mitchell HCS, Privacy and Discovery Program Manager

 360.725.2537 office

## introduction

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](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-05-01.pdf) and the [IT Security Policy 15.10](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-15-10.pdf). The rights of clients are described in [DSHS Administrative Policy 5.03](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-05-03.pdf)

**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).

* + “Unsecured PHI” is PHI that has not been made unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology such as encryption.

The Breach Rules apply to your partners and business associates as well – report any losses and compromises of PHI that are reported to you or that you discover.

**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 provides clients with specific rights regarding their PHI.

**HIPAA Rules:** Create safeguards for how we treat PHI.

PHI=Individually Identifiable Health Information (IIHI) about a Client that is transmitted or maintained by a DSHS HCC in any form or medium.

* + PHI includes demographic information that identifies the individual or about which there is a reasonable basis to believe it can be used to identify the individual.
1. We must safeguard PHI whether it is received, maintained, or communicated verbally, electronically or in writing.

**Privacy Rule:** Regulates the circumstances under which covered entities may use and disclose PHI and requires covered entities to have safeguards in place to protect the privacy of the information.

* + Demographic (name, address, DOB, SSN, Driver’s Lic #)
	+ Financial (credit card/bank acct #, claims info)
	+ Eligibility (client status; receiving public assistance)
	+ PHI (includes the above & clinical info – diagnosis, medications, lab results)

**Security Rule:** Requires covered entities to implement certain administrative, physical, and technical safeguards to protect electronic information.

* + Administrative Safeguard – Training
	+ Physical Safeguard –key card access
	+ Technical Safeguard - encryption

**Covered Entities:** The HIPAA Rules apply to **covered entities**, and to their business associates who perform functions or provide services for the covered entity.

* A covered entity is a
	+ **Health Plan**, (e.g. Medicaid)
	+ **Health Care Provid**er, (are covered by HIPAA if they transmit **electronic** health information in connection with certain transactions, such as billing and payment). Or a
	+ **Health Care Clearinghouse**, (There are no health care clearinghouses in DSHS).

**Hybridization:**

* May 3, 2013 – DSHS declared itself to be a “Hybrid Covered Entity” under HIPAA.

This means some DSHS programs are designated as Health Care Components or HCCs.

HCCs are covered by HIPAA and subject to HIPAA requirements (i.e. Privacy Rule, Security Rule and Breach Notification Rule).

**Minimum Necessary Concept:** RCW 70.02.260(9)

* + Consistent with the goals of the health information privacy provisions of [HIPAA, DSHS shall ensure] that the information disclosed is limited to the minimum necessary to serve the purpose for which the information is requested.
* Specifically it stands for the minimum amount of health information needed to accomplish
	+ the purpose of a request for health information

or

* + the use of health information needed to perform one’s job.

**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)

**Best Practices for Protecting Confidential Information**

* + Encrypt electronic devices
	+ Do not leave client information in a vehicle unattended
	+ Check email addressees 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

**When HIPAA does not apply**

* + HIPAA does not apply to employee information.
	+ Specifically in our capacity as “work force members.”
	+ Employee health information housed with employer though is exempt from disclosure.

**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

**De-identification Standards for HIPAA/HCIA**

1) Names 7) Health plan beneficiary numbers

2) Telephone numbers 8) Account numbers

3) Fax numbers 9) Certificate/license #s

4) Electronic mail addresses 10) Device identifiers & serial #s

5) Social security numbers 11) Web Universal Resource Locators(URLs)

6) Medical record numbers 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 Privacy Coordinators on the Privacy SharePoint site.)
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**

The second through fifth steps are my responsibility. I work with staff as necessary to immediately contain the breach. Some examples are:

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

Next, I work with staff on filling out the Privacy Breach Questionnaire. The questionnaire is important. Here is what I look for:

* General summary of what happened
* Start and end date of breach
* Discovery date of breach
* Number of affected individuals
* Type of breach occurred
* Improper disposal of PHI
* Mis-mailed
* Mis-emailed
* Loss
* Theft
* Unauthorized Access/Disclosure
* Where breach occurred
* Type of PHI involved
* Name
* Address
* SS#
* DOB
* Financial
* Clinical
* Other
* Mitigation Steps

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

The Risk Assessment is vital and required by HIPAA. The designated Privacy Coordinator for the HCC must complete the HIPAA breach risk assessment in the DSHS Privacy Breach Application (PBA) for any incident that is a potential Breach. Under HIPAA, a Breach is presumptive unless the HCC can document that there is a low probability that the PHI has been compromised. The Risk Assessment needs to be conducted quickly and as thorough as possible.

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.
3. 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**](http://www.dshs.wa.gov/pdf/ms/forms/03_387add.pdf)**.**

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). Here is what we look for:
2. Nature and extent of PHI involved, including types of identifiers and ability to identify individual. For example:
3. Information used elements that could be used for identity theft
4. Name or other unique identifiers tied with Social security numbers
5. Driver’s license numbers
6. financial account numbers with passwords
7. Nature of person who acquired, accessed, used or received the PHI: Example:
8. Limited or no risk of redisclosure of information by recipient.
9. Employee of another covered entity or business associate;
10. Recipient required by law to maintain confidentiality such as attorney/client privilege or law enforcement; recipient returned information;
11. Severe risk of disclosure
12. Acquisition was as a result of a criminal act including theft or hacking.
13. Risk whether PHI was actually accessed or acquired by unauthorized individual:
14. No proof of access or acquisition of PHI
15. Known or reported that access to PHI was acquired, used, sold, or further disclosed for malicious purposes.
16. Mitigation steps taken as a result of the breach: Example:
17. Verbally counseled responsible employee on HIPAA and administrative policies for managing the protection of PHI.
18. Reviewed LMS- DSHS Medical Information Privacy Training

**Step 4: NOTIFICATION**

The HIPAA Breach Notification Rule, requires Covered Entities and Business Associates to provide notification following a Breach of unsecured PHI. The notification requires certain language be included in the notification letter. Any notification letters required by HIPAA, must be reviewed and approved by the program’s designated Privacy Coordinator, or the DSHS Privacy Officer. Other laws that require notification include RCW 42.56.590 and RCW 70.02.290.

1. When to Notify Affected Individuals
	1. Notification must be made within 60 days of the date the breach is discovered.
2. How to Notify Affected Individuals
	1. Written notice must be sent via first-class mail to the affected individual at the last known address of the individual, or, if the individual agrees to electronic notice, by email.
	2. Deceased Individuals: 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.
3. Substitute Service
4. If the covered entity has insufficient or out-of-date contact information that precludes written notification, a substitute notice reasonably calculated to reach the individual shall be provided.
	1. Substitute notice is not required when the affected individual is deceased, but the covered entity has sufficient or out-of-date contact information for the next of kin or personal representative of the individual.
5. What must be Included in the Notification
6. Date of the breach
7. Description of the breach
8. Description of the information inappropriately accessed, or disclosed
9. Description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and to protect against any further breaches.
10. Steps the affected individuals can take to further mitigate the risk of harm
11. Contact info, to include toll free number, email address, website, or postal address

**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:

1. Equifax

www.equifax.com

1-800-548-7878

PO Box 740256

Atlanta, Georgia 30374

1. Experian

www.experian.com

1-888-397-3742

PO Box 9701

Allen, Texas 75013

1. TransUnion

www.transunion.com

1-800-680-7289

PO Box 2000

Chester, Pennsylvania 19076

**Others to Notify**

1. OCR
2. For breaches affecting less than 500 individuals, the Secretary of the U.S. Department of Health and Human Services (HHS) must be notified no later than 60 days after the end of the calendar year in which the breach was discovered.
3. For breaches affecting 500 or more individuals, covered entities must notify the secretary without unreasonable delay and in no event later than 60 days following discovery of 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 event later than 60 days following discovery of the breach.
1. AP Policy 2.07 requires press releases to go through the DSHS Office of Communications.
2. State Attorney General Office (RCW 42.56.590)
* Under 42.56.590(10) for any breach over 500, a covered entity must also notify the AGO.
* WA State AGO makes these notifications public on its website.

**Destruction or Return Requirement:**

If you receive health care information that you are not authorized to receive then you must destroy the information.

* + You may also return the health care information to the entity that provided the information if the entity is a health care facility or provider subject to Health Care Information Act (HCIA).

**Consequences for Breaches**

You have an obligation by law to protect the confidential client information you receive and maintain.

* Employees found to be in violation relating to confidentiality of PHI and other confidential information may receive corrective action, up to and including dismissal. Training and other mitigation steps may also be required. 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 10 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 and 164 (HIPAA Privacy Rule)

**Resources**

### Related RCWs and CFRs

[RCW 42.56](http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56) Public Records Act

[RCW 70.02](https://apps.leg.wa.gov/RCW/default.aspx?cite=70.02) Health Care Information

[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

**Related Administrative Policies**

[Administrative Policy 5.01](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-05-01.pdf) Privacy Policy -- Safeguarding Confidential Information
[Administrative Policy 5.03](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-05-03.pdf) Client Rights Relating to Protected Health Information

[IT Security Policy 15.10](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-15-10.pdf) Information and Technology Security

[Administrative Policy 2.07](http://one.dshs.wa.lcl/Policies/Administrative/DSHS-AP-02-07.pdf) Visual Communications Policy

**Related Links and Websites**

[HIPAA Privacy Training](http://hrd.dshs.wa.gov/Position_Management/Recruitment_and_Training_Support_Services/Employee_Agency_Training/Required_Agency_Training.htm) HIPAA Privacy Training

[HIPAA Covered Programs (HCC List)](http://www.dshs.wa.gov/pdf/ms/forms/03_387add.pdf) HCC List

[HIPAA Breach Notification Rule](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html) HIPAA Breach Notification Rule

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

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

Sample Letters and Forms

[**Sample 42-56-590 Client Notification**](http://one.dshs.wa.lcl/FS/Records/Privacy/Sample%20Letters/Sample%20RCW%2042-56-590%20Notification%206-1-18.doc)

[Privacy Breach Questionnaire](file:///C%3A%5CUsers%5CMitchCM%5CDesktop%5CMisc%5CSample%20Forms%5CPrivacy%20Breach%20Questionnaire.docx)

Contacts

[DSHS Privacy Coordinators](http://one.dshs.wa.lcl/FS/Records/Privacy/Breach/Breaches/DSHS%20Privacy%20Coordinators%205%202020.docx)

Acronyms

AGO Attorney General Office

AP Administrative Policy

HCC Health Care Component

HCIA Health Care Information Act

HIPAA Health Information Portability and Accountability Act
HHS Health and Human Services

IHH Individually Identifiable Health Information

IP Internet Protocol

LMS Learning Management System

OCR Office for Civil Rights

PBA Privacy Breach Application

PHI Protected Health Information

SS# Social Security Number

TOC Technology Operations Center

URL Universal Resource Locators

##