# Administrative Policy No. 5.01

**Subject:** Privacy Policy -- Safeguarding Confidential Information

**Information Contact:**

DSHS Privacy Officer
Office of Information Governance
MS: 45135, (360) 902-8278, FAX (360) 902-7848
E-mail: DSHSprivacyofficer@dshs.wa.gov

DSHS Chief Information Security Officer
Technology Innovation Administration MS: 45889
(564) 223-8617
E-mail: isoteam@dshs.wa.gov

**Authorizing Source:**

RCW 70.02 – Health Care Information Act
RCW 40.26.020 – Biometric Identifiers
RCW 42.56.590 – Personal Information – Notice of Security Breaches
Executive Order 16-01, Privacy Protection
HIPAA Rules – 45 CFR Parts 160, 162, and 164
DSHS Information Security Manuals

**Effective Date:** April 14, 2003

**Revised:** December 19, 2024 [1] housekeeping 01-16-2025 [2] Housekeeping 2/14/25 [3] Housekeeping 3/5/2026

**Approved By:** **Original approved by Pearlette J. Ramos**
Senior Director, Office of Justice and Civil Rights

---

## Purpose

This policy describes the commitment of the Department of Social and Health Services (DSHS) to vigorous privacy practices for safeguarding confidential 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

DSHS Official

threats, hazards, and inappropriate uses or disclosures.

**Scope**

This policy applies to all DSHS administrations, employees, interns, community compensation participants, and volunteers.

**Definitions**

**Biometric identifier:** Any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry, or other data generated by automatic measurements of an individual's biological characteristics, except when such information is derived from information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under HIPAA or other exclusions in RCW 40.26.020(7)(b)(i)-(iv).

**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.

**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.

**Business associate organizational units (BAOU):** BAOUs are internal to DSHS and perform activities that relate to providing health care. These activities must relate to covered functions. Some examples of covered functions include conducting quality assessment and improvement activities; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; legal, actuarial, accounting, consulting, data aggregation, management administrative, accreditation, or financial services, and other activities relating to the creation, renewal or replacement of a contract of health insurance, or health benefits. BAOUs are health care components covered by HIPAA and must comply with HIPAA rules when performing work on behalf of or associated with another DSHS health care component.

**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.

DSHS Official

**Client record:** Includes information held by or for DSHS that relates to a particular client.

**Confidential information:** Information that is protected by state or federal laws, including information about DSHS clients, employees, community compensation participants, volunteers, interns, vendors or contractors that is not available to the public without legal authority. For example, PHI is a type of client confidential information and personally identifiable information (PII) is a type of employee confidential information.

**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.

**Designated record set:** A group of records maintained by DSHS that are: a) medical records and/or billing records about clients; b) enrollment, payment, claims adjudication, and case or medical management records; or c) used, in whole or in part, to make decisions about clients. In DSHS, the designated record set may be a subset of the client record.

**Disclosure:** The release, transfer, or the providing of access to information outside of DSHS.

**Employee:** An individual to whom DSHS pays a salary, wages, or benefits for work performed for the DSHS who may have access to state vehicles, state issued mobile devices, or to whom DSHS provides reimbursement for tuition or miscellaneous expenses.

**DSHS privacy officer:** A person designated by the DSHS secretary or secretary's designee to oversee the DSHS privacy program.

**DSHS public records officer:** The person designated as the public records officer for the DSHS under RCW 42.56.580. The DSHS public records officer has primary responsibility for management, oversight and monitoring of DSHS 'Public records request process.

**DSHS privacy notice:** The DSHS website notice required by executive order 16-01 that addresses the collection, use and privacy of, and access to information that may be shared through the use of DSHS websites by clients and the public. Please see the DSHS privacy notice.

**Health care:** Care, services, or supplies related to the health of a client, including, but not limited to, preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care; counseling for a physical or mental condition, or a prescribed drug, device, or equipment.

**Health care component (HCC):** A component or combination of components of a hybrid covered entity designated by the hybrid covered entity as a health plan, a covered health care provider, or both. Health care component also means identified business associate

DSHS Official

organizational units (defined above).

**Health care provider:** A provider of medical or health services, and any person or organization that furnishes, bills, or is paid for providing health care in the normal course of business. A health care provider is a covered entity if it transmits information electronically in conjunction with a HIPAA standard transaction (See 45 CFR 160.103).

**Health care information act (HCIA):** Chapter 70.02 RCW medical records – health care information access and disclosure.

**Health information:** Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by DSHS concerning an identifiable individual;
2. Relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and
3. Identifies or can readily be associated with the identity of an individual. "health information" is also considered to be the same as "health care information" in the HCIA (RCW 70.02.010).

**Health plan:** An individual or group plan that provides or pays the cost of medical care or health related services, including government programs such as Medicare and Medicaid. This is the same as "third-party payor" as defined in the HCIA.

**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, which protects the privacy of individually identifiable health information; the HIPAA security rule, which sets national standards for the security of electronic protected health information; the HIPAA breach notification rule, which 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.

**HIPAA notice:** DSHS notice of privacy practices for client protected health information that is required by HIPAA.

**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.

DSHS Official

**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, such as, 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.

**Non-health care component (Non-HCC):** A component or combination of components of a hybrid covered entity that is not subject to HIPAA rules.

**Payment:** Payment applies to a broad range of activities that includes obtaining premiums, reimbursement, eligibility and coverage determinations, risk adjustment, billing and claims management coverage and utilization review activities, as well as disclosure to consumer reporting agencies of certain information.

**Personally identifiable information (PII) (also called personal information):** Personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. This includes demographic and financial information about a particular individual that is obtained through one or more sources such as name, address, social security number, driver's license number, client identification number, Washington identification card number, student, military, or passport identification number, health insurance policy number or health insurance identification number, any health information, biometric identifiers, full date of birth, e-mail address (especially in combination with user name and password or security questions and answers that would permit access to an online account), telephone number, account number, credit and debit card numbers and expiration dates, or any required security code, access code or password that would compromise an account, or any other numbers or information that can be used to access a person's financial account, electronic check numbers, case numbers, and financial account numbers connected with an electronic funds transfer, or a private key that is unique to an individual and that is used to authenticate or sign an electronic record. See RCW 42.56.590 and Executive Order 16-01.

**Privacy program:** DSHS's privacy program is developed to comply with federal and state privacy requirements. The individuals primarily responsible for implementing and operating this program are the DSHS privacy officer, the DSHS public records officer, the HIPAA security rule program manager, and designated privacy coordinators throughout DSHS, including DSHS institutions. The DSHS privacy program is responsible for carrying out adopted policies and procedures related to the privacy and security of confidential information.

**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

DSHS Official

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.

**Privacy coordinator:** A person designated by DSHS administrations, divisions, institutions, or regions to manage and direct privacy issues, client privacy rights, and to coordinate with the DSHS privacy officer in carrying out the DSHS's privacy program.

**Treatment:** The provision, coordination or management of health care and related services including the consultation between health care providers or the referral of a patient from one health care provider to another.

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

**Volunteer:** A person, who of their own free will, performs authorized duties for DSHS without expecting compensation or other benefits. DSHS does not pay wages or provide benefits but provides a volunteer reimbursement for actual expenses incurred in performing authorized duties.

**Website:** A collection of related web pages on the Internet to which a client or the public has direct access.

**Willful neglect:** The conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA rules. (See 45 CFR 160.401).

**Policy**

**A. Hybrid entity status**

DSHS is a hybrid entity that has designated programs as **health care components** (HCCs) within the administrations/divisions as provided on the DSHS website. As such, DSHS is a hybrid entity made up of both HCCs and Non-HCCs. Only DSHS HCCs, including business associate administrative units (BAOUs) are subject to the HIPAA rules.

Designation of HCC or Non-HCC status within DSHS is a formal process that involves program representatives and the designated privacy coordinators. The HCC designation process occurs every three years. HCC or non-HCC status may change due to programmatic changes or reorganization. Administrations are responsible for updating designations when programs functions change and for new programs or facilities. More information on the specific process is available on the privacy SharePoint site.

Designated health care components are not permitted to disclose protected health information to another component of the covered entity in circumstances prohibited by the HIPAA privacy rule. Under the privacy rule, it is as if the health care component and non-health care component are separate and distinct legal entities. (See 45 CFR

DSHS Official

164.105(a)(2)(ii)(A)).

**B. Assignment of administrative responsibilities**

1. **DSHS privacy officer**
The DSHS privacy officer provides oversight of the DSHS privacy program under Executive Order 16-01, "Privacy Protection and Transparency in State Government", which covers personally identifiable information, and the HIPAA Rules. The DSHS privacy officer works with the DSHS public records officer, chief information security officer, HIPAA security rule program manager, and the designated DSHS privacy coordinators to resolve privacy issues.

2. **Administration privacy coordinators**
Privacy coordinators help facilitate awareness of HIPAA in relevant health care components and assist in implementation of the DSHS privacy program, which includes carrying out DSHS policies and procedures related to the privacy and security of confidential information. At a minimum, each DSHS administration will have at least one designated privacy coordinator. Divisions, institutions, or regions may have additional designated privacy coordinators. Please see the DSHS privacy SharePoint site to determine designated agency privacy coordinators.

3. **DSHS chief information security officer**
The DSHS chief information security officer provides assistance to the DSHS privacy officer in administering the DSHS privacy program. The DSHS chief information security officer:
   a. Addresses information technology security issues;
   b. Is the designated security official for DSHS under 45 CFR 164.308(a)(2); and
   c. Maintains policies and procedures to address privacy and data security issues. See administrative policy 15.10 and DSHS information security manuals for details.

**C. Safeguarding confidential information**

By law, DSHS must safeguard confidential information that DSHS collects, uses, stores, and discloses. DSHS must properly safeguard confidential information of clients and others from inappropriate use and disclosure.

Employees must follow DSHS policies and procedures in the DSHS information security manuals 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.

Department contracts and agreements must contain confidentiality language and data

DSHS Official

security requirements approved by the chief information security officer. In addition, Business Associate contracts and their applicable downstream contracts must contain specific language addressing the business associate requirements under the HIPAA rules.

While the HIPAA Rules apply only to DSHS HCCs (including BAOUs), all administrations are expected to comply with applicable laws, follow best practices, and applicable department policies and procedures to safeguard confidential information.

The designated DSHS HCCs are specified on the public DSHS website as a part of the DSHS Notice of Privacy Practices. Documentation of the process used to determine HCC and BAOU designations can be found on the internal privacy SharePoint site.

**D. Collection and use of confidential information**

Social security numbers and other sensitive personally identifiable information (PII) and financial identifying numbers must not be collected unless necessary for agency operations and no other reasonable alternatives are available. Reasonable alternatives may include creating unique identifiers for clients using a combination of identifiers, which may include the last four digits of the social security number in combination with the first name, last name, date of birth, email, etc. DSHS must make reasonable efforts to limit the inclusion of social security numbers and other sensitive PII and financial information to the least amount necessary to accomplish the intended purpose when using or disclosing client confidential information. With respect to new information collected in the course of serving clients, DSHS must only collect the data required to fulfill the agency function or service to the client.

**E. Use, disclosure, and requests for PHI limited to minimum necessary**

1. DSHS health care components (HCCs) and their employees, community compensation participants, volunteers, and interns must make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary, to accomplish the intended purpose. The same efforts must be made when requesting PHI from another Covered Entity or its Business Associate.

2. The minimum necessary requirement covers uses of PHI within DSHS by HCCs and disclosures of PHI outside of DSHS except for disclosures:
   a. To a health care provider for treatment;
   b. Made to clients about themselves;
   c. Made according to a valid authorization;
   d. Made to the secretary of Department of Health and Human Services;
   e. Required or permitted by law. See examples in the notice of privacy practices.

3. Each DSHS HCC must develop and maintain the following information regarding

DSHS Official

access to and use of PHI:

a. Identify employees or the classification of employee who need access to PHI to perform their job functions;
b. The types of PHI to which access is needed and any conditions appropriate for employee access;
c. Written procedures to limit access to only the minimum amount of PHI needed to perform an employee's job.

**F. Collection and use of biometric identifiers**

1. Unless authorized by law, an administration may not collect or use biometric identifiers without first providing notice and obtaining consent of the individual. This includes clients, DSHS employees, DSHS contractors, vendors, interns, community compensation participants, and volunteers.

2. The notice and consent provided must clearly specify the purpose and use of the biometric identifier and must be retained for the duration of the retention of the biometric identifier.

3. Any biometric identifier obtained may not be sold and may only be used consistent with the terms of the notice and consent. That is, if an administration intends to share biometric identifiers with other governmental entities, the notice and consent must specify this use before sharing the information.

4. Biometric identifiers are not subject to public disclosure (see RCW 40.26.020(5)).

5. Biometric identifiers collected must be the minimum necessary to accomplish the purpose for collection and must not be retained longer than necessary to fulfill the original purpose and use, as specified in the notice and consent or as authorized by law.

6. Biometric identifiers must be stored and transmitted in compliance with the DSHS information security manuals' standards for Category 4 data.

7. Administrations or divisions having their own biometric identifier requirements must either follow or incorporate these requirements into their policies and procedures.

**G. Confidential information on a website**

1. When DSHS gives information about client services or benefits on a website must be posted and made available electronically. See administrative policy 15.18.02

2. Executive Order 16-01 requires access to the DSHS privacy notice from each home page website and a link to the DSHS privacy notice on any page on the

DSHS Official

website that collects data from individuals. See administrative policy 15.18.02.

3. Administrations that collect confidential informational on their websites must have links to the DSHS privacy notice on the first web page and any web page that collects confidential information.

The HIPAA notice of privacy practices (NPP) is required to be posted on the DSHS public website homepage. See 45 CFR 164.520(c)(3)(i).

**H. Breaches or potential breaches of confidential information.**

1. Reporting:

If a breach or potential breach of confidential information is discovered, staff at a minimum must notify within one (1) business day of discovery:

a. The technology operations center (TOC) at ETOC@dshs.wa.gov; and
b. The administration's or division's privacy coordinator. (Please see privacy coordinators the privacy SharePoint site.)
c. 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.

Administrations or divisions having their own incident reporting requirements or policies for reporting breaches or potential breaches must follow and incorporate these reporting requirements into their procedures.

2 Breach Risk Assessment

a. HIPAA - health care components (HCCs):
   i. 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 presumed unless the HCC can document that there is a low probability that the PHI has been compromised. 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.
   ii. The designated privacy coordinator for the HCC must complete the HIPAA breach risk assessment in the 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.
b. RCW 42.56.590 Personal Information. The designated privacy coordinator must determine if client personal information, as defined in the law, is

DSHS Official

reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured.

3. 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.

## I. Mitigation

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.

## J. Designation of a record set

Each health care component must define the types or sources of information or records included in its designated record set. See the DSHS designated record set on the privacy SharePoint site.

## K. Retention of confidential information

DSHS programs within DSHS administrations must regularly examine their record retention schedules to ensure that confidential information collected by DSHS is only kept long enough to accomplish the purpose of the collection or as long as required by law.

DSHS health care components must maintain the following HIPAA privacy documentation for a minimum of six years from the date of creation or the date when last in effect, whichever is later:

1. Privacy policies and procedures.

2. Any written requests or documentation of action or activity relating to clients exercising their privacy rights (See administrative policy 5.03, section C).

DSHS Official

3. Titles of the privacy coordinators responsible to receive and process a client's request to:
   a. Access and copy PHI;
   b. Receive alternative communication regarding PHI;
   c. Restrict the use and disclosure of PHI;
   d. Amend PHI; or
   e. Receive an accounting of disclosures of their PHI.

4. Clients' authorizations for the use or disclosure of PHI.

5. Notice of privacy practices.

6. Privacy complaints and their disposition.

7. Documentation that employees have completed HIPAA privacy training.

8. Breach risk assessments and reporting.

9. Other documents required by the HIPAA Rules, including the Security Rule risk analyses or risk assessments.

**L. Privacy training**

All DSHS employees, interns, and volunteers must receive HIPAA privacy training related to the use, disclosure, and collection of PHI. Training must be documented either in the learning center or in the employee's personnel file. The HIPAA training is mandatory and must be taken at least every three years.

New employees must receive HIPAA privacy training within thirty (30) calendar days after being employed by DSHS. See DSHS's learning center resource page managed by the human resources division.

Employees of HCCs must also take additional available training addressing HIPAA compliance. Privacy coordinators must also receive HIPAA and other confidentiality training.

All DSHS employees, volunteers, and interns must also receive annual security training as required by the information security standards manual.

**M. Privacy complaints**

1. Individuals believing that DSHS has violated a client's privacy rights relating to PHI or who have complaints concerning DSHS policies or procedures required by HIPAA or compliance with policies and procedures required by HIPAA (45 CFR

DSHS Official

164.530(d)) may file a written complaint with either:

a. The DSHS privacy officer at DSHSprivacyofficer@dshs.wa.gov; or

b. The secretary of the Department of Health and Human Services (DHHS) Office for Civil Rights, or both. See filing a complaint on the HHS.gov website.

2. Individuals believing that DSHS has violated a person's general privacy rights (not related to PHI and for part of DSHS that is not a health care component) may file a written complaint with the DSHS privacy officer.

3. The DSHS privacy officer in coordination with the appropriate designated privacy coordinator(s) will be responsible for investigating and resolving privacy complaints. If complaints or breach incidents involve DSHS personnel, all applicable personnel policies must be followed.

4. All Office for Civil Rights reporting and communication regarding HIPAA and privacy issues (excluding complaints), including the U.S. Department of Health and Human Services Office for Civil Rights (OCR) transactions and investigations, must be coordinated with the DSHS privacy officer. The DSHS privacy officer must be informed within one (1) business day of any contact by OCR to DSHS or its employees regarding matters pertaining to the HIPAA rules.

**N. 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.

State laws applicable to DSHS programs including RCW 74.04.060, RCW 74.34.040, Chapter 13.50 RCW, Chapter 10.77 RCW; and Chapter 70.02 RCW) and federal regulations (including HIPAA rules, the Social Security Act, and substance use disorder rules in 42 CFR, Part 2) prohibit unauthorized access, use, or disclosure of confidential information. These laws may impose other sanctions, fines, and penalties.

**Note:** The Attorney General's Office will provide state officers, employees, and other covered persons with legal defense for actions or claims instituted against such persons arising out of activities performed in good faith within the scope of their duties. For additional information please see the DSHS discovery manager SharePoint site, AGO lawsuits against the state and the state employee, and

DSHS Official

DSHS administrative policy 5.05 management of the litigation discovery process.

**O. Actions prohibited against those reporting privacy violations**

DSHS is prohibited by state and federal law from intimidating, threatening, coercing, discriminating against or taking any other retaliatory action toward an individual based on their filing of a privacy complaint.

In addition, DSHS may not require clients to waive their right to file a privacy complaint as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

**P. Compliance reviews**

DSHS recognizes the right of the secretary of the Department of Health and Human Services to conduct compliance reviews of DSHS when a preliminary review of facts indicates a possible violation of HIPAA due to "willful neglect." (See 45 CFR 160.306 and 45 CFR 160.308). Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA.

In the case of a compliance review of DSHS for violations for willful neglect, DSHS must correct the violation within thirty (30) days. The 30-day period begins on the first date DSHS knew or by exercising reasonable diligence would have known that a violation occurred. Depending on the scope and nature of the violation, DSHS will form an incident response team to correct the violation.

---

[1] Housekeeping to remove community compensation participant from training section.
[2] Housekeeping to update link for security manual section C.
[3] Fixed broken links throughout.

DSHS Official