Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 5.01

Subject: Privacy Policy -- Safeguarding Confidential Information

Information Contact:

DSHS Privacy Officer
Office of Policy and External Relations
MS: 45115, (360) 902-8278, FAX (360) 902-7848
E-mail: DSHSprivacyofficer@dshs.wa.gov

DSHS Chief Information Security Officer
Information System Services Division
MS: 45889, (360) 902-7679
E-mail: CISO@dshs.wa.gov

Authorizing Source:

RCW 70.02 – Health Care Information Act
RCW 42.56.590 RCW – Public Records Act
Executive Order 00-03, Public Records Privacy Protections
HIPAA Rules – 45 CFR Parts160, 162, and 164 HITECH Act
Information Technology Security Policy Manual
Information Technology Procedures Manual

Effective Date: April 14, 2003

Revised: January 12, 2015

Approved By: **Original signed by Dana Phelps**
Senior Director, Policy & External Relations

Purpose

This policy describes the Department of Social and Health Services' (DSHS or Department) dedication to vigorous privacy practices for safeguarding Client Confidential Information, which includes Protected Health Information (PHI), to:

- Promote responsible information management practices by administrations;
- Promote public trust and confidence in the use of online services or other services provided by the Department;
- Protect the privacy rights of Clients when DSHS uses, obtains, maintains, or discloses Client Confidential Information; and
- Maintain the confidentiality, integrity, and availability of PHI while protecting

against any reasonably anticipated threats, hazards, and/or inappropriate Uses or Disclosures.

Scope

This policy applies to all DSHS administrations, Employees, and Volunteers.

Definitions

Breach: The acquisition, access, Use, Disclosure, or loss of Confidential Information in a manner not permitted by state and federal law.

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 the Department's daily 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 covered by HIPAA when performing work associated with a 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, parents and children involved with child welfare services, juveniles involved with the juvenile justice system, 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: Personal Information, including PHI, which identifies a Client, and that state or federal laws protect from improper Disclosure or Use.

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, vendors or contractors that is not available to the public without legal authority. For example, PHI is a type of Client Confidential Information.

Covered Entity: A Covered Entity is a Health Plan, a health care clearinghouse, or a Health Care Provider. 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). As defined in 45 CFR 164.103, DSHS is a Hybrid Covered Entity that has designated programs as Health Care Components within the administrations/divisions as provided on the DSHS Website. DSHS is a Hybrid Covered Entity with only its Health Care Components and identified BAOUs 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 DSHS pays a salary, wages, or benefits to for work performed for the department who may have access to the SCAN, state vehicles, state issued pagers, Personal Digital Assistants (PDA), or cell phones, 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 Department's Privacy Program.

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

DSHS Security Notice: The DSHS website notice required by Executive Order 00-03 that addresses the collection, use and security of, and access to information that may be shared through the use of DSHS websites by Clients and the public. Please see the DSHS Security 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 Components also means identified Business Associate 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 a Client or potential Client; and
2. Relates to the past, present, or future physical or mental health or condition of the individual; the provision of Health Care to the individual; or the past, present, or future Payment for the provision of Health Care to the individual; and
3. Identifies or can readily be associated with the identity of a Client or potential Client. "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, or government program that provides or pays the cost of medical care or health related services provided by Department covered Health Care Components or other Covered Entities as defined by HIPAA. 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 and Breach Notification Rules.

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 confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

HIPAA Notice: DSHS Notice of Privacy Practices for Client Protected Health Information that is required by HIPAA.

Hybrid Covered Entity: A single legal entity:

1. That is a Covered Entity;
2. Whose business activities include both covered and non-covered functions; and

That designates Health Care Components in accordance with the Privacy Rule. The Department is a Hybrid Covered 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, 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.

Personal Information (also called Personally Identifiable Information or PII): Personal Information means exempt demographic and financial information about a particular individual that is obtained through one or more sources. This normally includes information such as name, address, social security number, driver's license number, e-mail address, telephone number, credit and debit card numbers and expiration dates, electronic check numbers, case numbers, and financial account numbers connected with an electronic funds transfer. See Executive Order 00-03.

Privacy Program: The Department'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 (as backup) and designated Privacy Coordinators throughout the Department, including Department institutions. The Department's Privacy Program is responsible for carrying out Department 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 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 Department'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 his or her own free will, performs authorized duties for the department without expecting compensation or other benefits. The department 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 administrative simplification provision violated in HIPAA. (See 45 CFR 160.401).

Policy

A. Hybrid Covered Entity Status:

DSHS is a Hybrid Covered Entity which has designated programs as Health Care Components (HCCs) within the administrations/divisions as provided on the DSHS Website. As such, DSHS is a Hybrid Covered Entity made up of both HCCs and Non-HCCs. Only the Department's HCCs and associated BAOUs are subject to the HIPAA Rules.

Designation of HCC or Non-HCC status within the Department is a formal process that involves program representatives and the designated Privacy Coordinators. Administrations are responsible for keeping designations current. HCC or Non-HCC status may change due to programmatic changes or reorganization. More information on the specific process is available on the Privacy SharePoint site.

B. Assignment of Administrative Responsibilities

1. **DSHS Privacy Officer**

The DSHS Privacy Officer provides oversight of the Department's Privacy Program under Executive Order 00-03-Public Records Privacy Protection, which covers Personal Information, and the HIPAA Rules. The DSHS Privacy Officer works with the DSHS Public Records Officer, Chief Information Security Officer, and the designated Department 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 Department's Privacy Program which includes carrying out Department 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 Department's 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 Department's Privacy Program. The DSHS Chief Information Security Officer:

a. Addresses information technology security issues;
b. Is the designated security official for the Department 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 IT Security Manuals for details.

B. Collection of Confidential Information

Social Security Numbers and other sensitive personal 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 or using a combination of identifiers, which may include the last four digits of the SSN in combination with the first name, last name, date of birth, email, etc.

C. 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.

D. Safeguarding the Confidentiality of Client Information

By law, DSHS must safeguard Client Confidential Information that includes demographic, financial, eligibility, and PHI collected, used, stored and disclosed by DSHS. The Department must properly safeguard Confidential Information of Clients from inappropriate Use and Disclosure.

Employees must follow DSHS policies and procedures in the DSHS Information Technology Security Policy Manual, the Information Technology Procedures Manual, and the Information Technology Standards Manual for handling Confidential Information.

Department contracts and agreements must contain confidentiality language 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 Privacy Rule.

While the HIPAA Rules apply only to DSHS Health Care Components and associated BAOUs, all administrations are expected to follow best practices and applicable Department policies and procedures to safeguard Confidential Information.

The designated DSHS Health Care Components are specified on the public DSHS Website as a part of the DSHS Notice of Privacy Practices. Documentation of the process used to determine Health Care Component and Business Associate Organizational Unit designations can be found on the internal Privacy SharePoint site.

E. Confidential Information on a Website

1. When DSHS gives information about Client services or benefits on a Website, the DSHS Security Notice must be posted and made available electronically. See Administrative Policy 15.18.02.

2. Executive Order 00-03 requires access to the DSHS Security Notice on each home page Website and a link to the DSHS Security Notice on any page on the Website that collects data from individuals. See Administrative Policy 15.18.02.

3. Administrations that collect Confidential Information on their Websites must have links to the DSHS Security Notice on the first web page and any web page that collects Confidential Information.

4. The HIPAA Notice (also called the Notice of Privacy Practices) is required to be posted on the DSHS public Website homepage. See 45 CFR 164.520(c)(3)(i).

F. Privacy Training

All DSHS Employees and Volunteers must receive HIPAA privacy training related to the Use, Disclosure, and collection of PHI. Training must be documented either in the Learning Management System (LMS) or in the Employee's personnel file.

New Employees must receive HIPAA privacy training within thirty (30) calendar days after being employed by DSHS. See the Department's LMS 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 and Volunteers must also receive annual security training as required by the IT Security policies.

G. Retention of Confidential Information

DSHS programs within Department 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);

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.

H. Use, Disclosure, and Requests for PHI Limited to Minimum Necessary

1. DSHS Health Care Components and their Employees and Volunteers must make reasonable efforts to limit the Use or Disclosure of PHI to the Minimum Necessary, to accomplish the intended purpose or when requesting PHI from another Covered Entity.

2. The Minimum Necessary requirement covers uses of PHI within DSHS by Health Care Components and Disclosures of PHI outside of DSHS except for Disclosures:
   a. To a Health Care Provider for Treatment;
   b. Made to a Client about themselves;
   c. Made according to an 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 Health Care Component must develop and maintain the following information regarding access to and Use of PHI:
   a. A current list of Employees or the classification of Employees 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.

I. Use and Disclosure of Social Security Numbers and Personal Information

DSHS must make reasonable efforts to limit the inclusion of social security numbers and other sensitive personal and financial information to the least amount necessary to accomplish the intended purpose when Using or Disclosing Client Confidential Information.

J. 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 164.530(d)) may file a written complaint with:
    a. The DSHS Privacy Officer at DSHSprivacyofficer@dshs.wa.gov; and/or
    b. The Secretary of the Department of Health and Human Services (DHHS) Office for Civil Rights. See How To File 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 an agency 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 OCR transactions and investigations, must be coordinated with the DSHS Privacy Officer. The DSHS Privacy Officer must be informed within one business day of any contact by OCR to DSHS or its employees regarding matters pertaining to the HIPAA Rules.

K. 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 (1) one business day of discovery:

a. The ISSD Service Desk at ISSDservicedesk@dshs.wa.gov; and
b. The administration's or division's Privacy Coordinator. (Please see Privacy Coordinators on 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. Notification:

If notification may be necessary as a result of a Breach of Client Confidential Information, Employees must contact their administration or division Privacy Coordinator. Depending on what laws apply, the notification may require certain language be included in the notification letter and when the letter must be sent. Any notification letters required by HIPAA must be reviewed and approved by the program's designated Privacy Coordinator, or the DSHS Privacy Officer or their designees. Other laws that require notification include RCW 42.56.590 and RCW 70.02.290.

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

3. HIPAA Breach Risk Assessment for Health Care Components:

a. If an incident of a potential Breach is determined not to be a Breach, the HCC must complete the HIPAA Breach Risk Assessment Form 23-040. Under HIPAA a Breach is presumptive unless the HCC can document that there is a low probability that the PHI has been compromised. Form 23-040 applies the four part test required by HIPAA to adequately document the determination that the incident is not a Breach.

b. The HIPAA Breach Risk Assessment form must also be completed for incidents that are determined to be a HIPAA Breach along with the DSHS Security Breach Report form, which is available on the Privacy SharePoint site or from the DSHS Privacy Officer.

L. Corrective/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 Department programs including RCW 74.04.060, Chapter 13.50 RCW; and Chapter 70.02 RCW) and federal regulations (including HIPAA Rules, the Social Security Act, and chemical dependency rules at 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 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 Administrative Policy 5.05 Management of the Litigation Discovery Process.

M. Compliance Reviews.

The Department recognizes the right of the Secretary of the Department of Health and Human Services to conduct compliance reviews of the Department 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 the Department for violations for Willful Neglect, the Department must correct the violation within thirty (30) days. The 30-day period begins on the first date the Department knew or by exercising reasonable diligence would have known that a violation occurred. Depending on the scope and nature of the violation, the Department will form an incident response team to correct the violation.

N. 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.

O. 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 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.