

Administrative Policy No. 5.06

Subject:	Use of Health Care Information Application of Chapter 70.02 RCW
Information Contact:	DSHS Privacy Officer Office of Information Governance MS: 45135, (360) 902-8278, FAX (360) 902-7848 E-mail: DSHSprivacyofficer@dshs.wa.gov
Authorizing Source:	Chapter 70.02 RCW – Health Care Information Act Chapter 434 WAC
Effective Date:	December 8, 2014
Revised:	May 1, 2022
Approved by:	<u>Original signed by Dana Phelps</u> Senior Director, Office of Policy and Rules

Purpose

This policy describes the Department of Social and Health Services' (DSHS or department) dedication to safeguarding health care information through vigorous privacy practices for that:

- Promote responsible information management practices by administrations; and
- Protect the privacy rights of clients when DSHS obtains or discloses Health Care Information.

Scope

This policy applies to all non-health care components within DSHS.

Definitions

Business Associate Organizational Unit (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; studies related to improving case management and care coordination;

contacting health care providers and patients with information about treatment alternatives; licensing activities, claims processing, data analyses, utilization review, patient safety activities; 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.

Health Care Component: 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, or a BAOU.

Health Care Facility: A hospital, clinic, nursing home, laboratory, office, or similar place where a health care provider provides health care to patients.

Health Care Information: Any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid (DNA) and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information.

Health Care Information Act (HCIA): Chapter 70.02 RCW – Medical Records – Health Care Information Access and Disclosure.

Health Care Provider: A person who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as modified by the American Recovery and Reinvestment Act of 2009 (“ARRA”), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

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
3. That designates Health Care Components in accordance with the Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164.

Non-covered Health Care Provider (NCHCP): 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 who does not use electronic media to transmit health information to perform HIPAA covered transactions. For example, a social service worker whose activities meet the HIPAA

definition of furnishing health care will be a health care provider but will not be subject to HIPAA if that social service worker does not transmit health information in an electronic form in connection with a transaction covered by HIPAA. The “non-covered” term means not covered by HIPAA.

Policy Requirements

A. Hybrid Covered Entity Status:

DSHS is a covered entity, which has designated programs as health care components within the administrations and divisions. These health care components are provided as an attachment to the DSHS Notice of Privacy Practices. As such, DSHS is a hybrid covered entity with only its [Health Care Components](#) subject to the HIPAA rules. Areas that are not subject to the HIPAA rules are non-health care components or non-HCCs.

B. Non-Covered Health Care Providers and Health Care Information

Under HIPAA, a DSHS HCC or another HIPAA covered entity may disclose protected health information to a NCHCP for treatment and payment activities. 45 CFR §506(c)(2) and (3). A NCHCP must use, create, transmit, and maintain health care information in compliance with chapter 70.02 RCW, the Uniform Health Care Information Act, and any other applicable state or federal laws and rules.

C. Treatment of Health Care Information:

This policy is based on the requirements of RCW 70.02.290. That section requires all state or local agencies obtaining health care information pursuant to RCW 70.02.050 and 70.02.200 through 70.02.240, that are not health care facilities or health care providers, to adopt a policy available on the department’s web site. That policy must establish (1) a reasonable notification period and (2) what information must be included in the notification if health care information is mistakenly received and later wrongfully disclosed as defined by RCW 70.02.290.

Department programs that receive health care information pursuant to RCW 70.02.050 and 70.02.200 through 70.02.240 must comply with the requirements below if the programs (1) are not health care facilities or health care providers; (2) have not requested a person’s health care information; and (3) are not authorized to receive that person’s health care information:

- a. Not use or disclose this information unless permitted under chapter 70.02 RCW; and
- b. Destroy the information in accordance with disposition authority number (DAN) GS 50004(set forth below) or return the information to the entity that provided

the information if the entity is a health care facility or health care provider and subject to the Health Care Information Act.

DESCRIPTION OF RECORDS	DISPOSITION AUTHORITY NUMBER (DAN)	RETENTION AND DISPOSITION ACTION	DESIGNATION
<p>General Information – External Information received from other agencies, commercial firms, or private institutions, which requires no action and is no longer needed for agency business purposes. Includes, but is not limited to:</p> <ul style="list-style-type: none"> • Catalogs, reports, multi-media presentations (videos, CDs, etc.); • Informational copies, notices, bulletins, newsletters, announcements; • Unsolicited information (junk mail, spam, advertisements, etc.). 	<p>GS 50004 Rev. 0</p>	<p>Retain until no longer needed for agency business <i>then</i> Destroy.</p>	<p>NON-ARCHIVAL NON-ESSENTIAL OFM</p>

D. Example scenario of when Policy 5.06 would apply:

Program A receives health care information regarding a client from ABC Clinic. Within the records are unrelated medical records regarding someone else wholly unaffiliated to the client and program.

Correct action: Program A realizes ABC Clinic’s mistake and either returns the unrelated medical records to the clinic or informs the clinic of the mistake and destroys the records.

Incorrect action which triggers notification: Program A does not notice the unrelated records and makes them part of a client’s file. Program A then receives a request for that client’s file and discloses it to the client, personal representative, etc. Program A becomes aware that the unrelated medical records were disclosed in error. Program A must notify the individual of the breach of their information.

E. Notification:

A person, about whom Health Care Information has been improperly disclosed, must be informed of the disclosure by the non-HCC or HCC improperly making the disclosure.

Notification must be provided within 60 days of discovery, which must include:

1. A brief description of what happened, including the date of the disclosure and the date of the discovery of the disclosure, if known.
2. The name of the entity that originally provided the information to the department must be included.
3. A description of the types of Health Care Information that were involved in the disclosure (such as whether full name, social security number, date-of-birth, home address, account number, email address, diagnosis, disability code, or other types of information involved including demographics).
4. Any steps individual should take to protect themselves from potential harm resulting from the disclosure.
5. A brief description of what the non-health care component or health care component involved is doing to investigate the disclosure, to mitigate harm to individuals, and to protect against any further disclosures; and
6. Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, email address, web site, or postal address.
7. The notification should also meet the plain talk requirements of the department to the extent possible.

F. Related Policies

Please refer to Administrative Policy 5.01 for additional information regarding notification and reporting breaches within the Department of Social and Health Services.