WASHINGTON STATE
Department of
Children, Youth, and Families

Administrative Policy

Chapter 13 Forms, Policies & Rules
13.04 Protecting Privacy and Confidential Information

Original Date: July 18, 2018
Revision Date: August 24, 2021
Sunset Review Date: August 31, 2024
Approved by: Frank Ordway, Chief of Staff

Purpose

The purpose of this policy is to:

- Safeguard the privacy of individuals.
- Protect client information that is collected, used, maintained, or disclosed by DCYF from misuse or unauthorized release.
- Promote responsible information management practices.

Scope

This policy applies to DCYF employees, volunteers, interns, and work study students.

Laws

Chapter 13.50 RCW	Keeping and Release of records by juvenile justice or care agencies
Chapter 26.44 RCW	Abuse of children
Chapter 40.14 RCW	Preservation and destruction of public records
RCW 40.26.020	Biometric identifiers-Notice and consent-Agencies-Use, storage, retention-Review-Definitions-Exceptions
RCW 43.17.410	Sensitive personal information of in-home caregivers for vulnerable populations-Release of information prohibited
RCW 42.56.230(2)	Personal information [of children enrolled in child care]
RCW 42.56.590	Personal information-Notice of security breaches
RCW 42.56.640	Vulnerable individuals, in-home caregivers for vulnerable populations
RCW 42.56.645	Release of public information-2017 c 4 (Initiative Measure No. 1501) [pertaining to in-home caregivers]
Chapter 70.02 RCW	Medical records-Health care information access and disclosure
RCW 74.04.060	Records, confidential-Exceptions-Penalty
RCW 74.13A.065	Records-Confidentiality.
RCW 74.13B.020(10)	Family support and related services-Performance based contracting.
Executive Order 16-01	Privacy Protection and Transparency in State Government
Title 7 U.S. Code § 1758	Program Requirements
Title 20 U.S. Code § 1232g	Family educational and privacy rights
Title 20 U.S. Code § 1439	Procedural safeguards (Individuals with Disabilities Education Act

	(IDEA Part C)).
Title 42 U.S. Code § 5106a	Grants to States for child abuse or neglect prevention and treatment programs
Title 42 U.S. Code § 671	State plan for foster care and adoption assistance
PL 104-191	Health Insurance Portability and Accountability Act (HIPPA) of 1996

Policy

1. DCYF must:
    a. Prominently display this policy on the DCYF website home page and on any other page where personal information is collected or viewable.
    b. Notify individuals who may be affected by a breach of the security of the system as described in RCW 42.56.590.
    c. Continually review and update this policy to align with current information collection and retention procedures.
    d. Verify employee training is documented in the Washington State Learning Center (WSLC) or in the employee's personnel file.
    e. Verify employees and individuals with access to confidential DCYF data submit a signed Nondisclosure of Confidential Information DCYF 03-374F form and an Agreement on Nondisclosure of Confidential Information-Non Employee DCYF 03-374B at the date of hire or data access and annually thereafter.
    f. Not intimidate, threaten, coerce, discriminate against or take other retaliatory actionstoward employees filing a privacy complaint.
    g. Not require clients to waive their right to file a privacy complaint as a condition of eligibility for services and benefits.
    h. Biometric Identifiers
        i. Inform and obtain consent from clients, DCYF employees, volunteers, interns, contractors, and vendors prior to collecting or using their biometric identifiers, unless authorized by law. The notice and consent must:
            A. Clearly specify the purpose and use of the biometric identifier.
            B. Be retained for the duration of the retention of the biometric identifier.
        ii. Verify biometric identifiers are not:
            A. Sold or given away, and may only be used as permitted by the terms of the notice and consent.
            B. Retained longer than the minimum time necessary to accomplish the purpose for collection.
            C. Disclosed per chapter 42.56 RCW, and stored and transmitted in compliance with the OCIO security standards for Category 4 data. See DCYF Administrative 12.04 Acceptable Use of Technology Resources and the Internet policy.
2. Employees, volunteers, and interns:
    a. Must:
        i. Complete the DCYF Information Security Awareness Training located in the WSLC related to the use, disclosure, and collection of confidential information.
        ii. Safeguard confidential information from inappropriate use and disclosure. This information includes:
            A. Demographics
            B. Financial
            C. Eligibility
            D. Medical
            E. Mental health
            F. Substance use disorder information collected, used, stored and disclosed by

DCYF

iii. Retain information only as long as needed to carry out the purpose for which it was collected and according to applicable retention schedule requirements.
iv. Make reasonable efforts to limit the inclusion of social security numbers (SSNs) and other personal and financial information in the records.
v. Dispose of records containing confidential information, per document retention standards, so the information is properly safeguarded.
vi. Comply with the Health Insurance Portability and Accountability Act (HIPAA) when handling protected health information.
vii. Notify the privacy officer and the DCYF IT Security Office within one business day of discovering a breach or potential breach of personal information.

b. May collect and use confidential information necessary for DCYF operations.

3. Divisions and offices must regularly examine their record retention schedule requirements to verify the information collected by DCYF is only kept long enough to accomplish the business need or as allowed by law.
4. The Chief Information Security Officer (CISO) or designee must:
   a. Collect confidential information, e.g., SSNs and other sensitive personal and financial identifying numbers, only when:
      i. It is required by law or it is necessary for DCYF operations.
      ii. There is no other reasonable alternative, e.g., creating unique identifiers or using a combination of client identifiers, including the use of the last four digits of the SSN in combination with the first name, last name, date of birth, e-mail, etc.
   b. Perform random sampling and periodic reviews of user access and user activity in FamLink or other applications potentially containing Social Security Administration (SSA) provided information.
   c. Take the following action, if there is a security incident that includes SSA provided information:
      i. Notify the DCYF official or designee responsible for the systems security designated in the Information Exchange Agreement (IEA). This information is available from the DCYF Contracts Unit.
      ii. The DCYF official or designee must notify the SSA Regional Office or the SSA systems security contact within one hour. If they cannot make contact within this timeframe, they must contact the SSA National Network Service Center (NNSC) at 1-877-697-4889. Select “Security and PII Reporting” from the options list. The Electronic Information Exchange Procedures (EIEP) will provide updates as they become available to SSA contact, as appropriate.
5. The privacy officer must:
   a. Investigate and resolve complaints from individuals who submit a written complaint to the privacy officer alleging that DCYF has violated a client’s privacy rights.
   b. Notify the Office of the Attorney General of any breach of confidential information involving or potentially involving over 500 individuals within 30 calendar days.
   c. Track and coordinate written or electronic notification to clients whose confidential information is disclosed per RCW 42.56.590 and RCW 70.02.290.

Definitions

Biometric Identifier means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, Deoxyribonucleic Acid (DNA), or scan of hand or face geometry, 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 of Data means the acquisition, access, use, disclosure, or loss of confidential information in a manner not permitted by state or federal laws.

Breach of Systems means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

Clients are individuals who are the beneficiaries of services or benefits from DCYF. This term includes but is not limited to, consumers, recipients, applicants, parents, youth, and children involved with DCYF. Clients include individuals who previously were the beneficiaries of services or benefits and persons applying for benefits or services.

Confidential Information is information that is protected by state or federal laws, including information about DCYF clients, employees, volunteers, interns, work study students, vendors, or contractors that is not available to the public without legal authority. This includes client records. Information is categorized into the following four areas:

- Category 1: Is public information that can be released to the public. It does not need protection from unauthorized disclosure, but doesneed protection from unauthorized changes that may mislead the public.
- Category 2: Is sensitive information that is not specifically protected by law, but is limited to official use only, and protected against unauthorized access. This data is available through public disclosure requests.
- Category 3: Is confidential information that is specifically protected by law and not available through public disclosure requests. It includes:
    - Personal information about clients, regardless of how the information is obtained. RCW 42.56.590 and RCW 19.255.010.
    - Information concerning employee payroll and personnel records per RCW 42.56.250.
    - Lists of individuals for commercial purposes as defined in RCW 42.56.070(8).
    - Sensitive personal information of family child care providers per RCW 43.17.410, RCW 42.56.640, and RCW 43.216.089.
    - Information about the infrastructure and security of computer andtelecommunication networks as defined in RCW 42.56.420.
- Category 4: Is confidential information that requires special handling, including but not limited to:
    - Protected Health Information (PHI), per DCYF Administrative13.04 Protecting Privacy and Confidential Information policy.
    - Information that identifies a person as being or ever having been a client of an alcohol or substance abuse treatment, or mental health program.
    - Federal wage data.
    - Location of an abused spouse.
    - Data that would compromise the agency's constituents.

Disclosure means the release, transfer, or the providing of access to information outside of DCYF.

Employees are individuals to whom DCYF pays salaries, wages, or benefits for work performed for DCYF.

Health Information is any information, whether oral or recorded in any form or medium that is

created or received by DCYF concerning a client or potential client; and relates to the past, present, or future physical, mental health or the past, present or future payment for the provision of health care to the individual; and identifies or can readily be associated with the identity of a client or potential clients "health information" is also considered to be the same as "health care information" in the Health Care Information Act per RCW 70.02.010.

Interns are individuals performing authorized work-related duties for DCYF to gain knowledge and hands-on work experience in state government. Internships may be paid or unpaid.

Personal Information means:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements:
    - Social security number (SSN) or the last four numbers of SSN.
    - Driver's license number or Washington identification card number.
    - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account.
    - Full date of birth.
    - Private key that is unique to an individual and that is used to authenticate or sign an electronic record.
    - Student, military, or passport identification number.
    - Health insurance policy number or health insurance identification number.
    - Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.
    - Biometric identifier data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.
- Username or email address in combination with a password or security questions and answers that would permit access to an online account.
- Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:
    - Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable.
    - The data element or combination of data elements would enable a person to commit identity theft against a consumer.
- Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Records are any documents or recorded information regardless of physical form or characteristics created, sent, organized, or received by DCYF in the course of public business including paper documents, emails, log books, drawings, graphs, charts, video or audio recordings, photographs, phone records, data compilations, planners, calendars, text messages, draft documents, electronically stored information (ESI), and metadata.

Security Incident is an event that has a significant impact on the agency IT resources or agency data.

Forms

Agreement on Nondisclosure of Confidential Information DCYF 03-374B
Nondisclosure of Confidential Information DCYF 03-374F (located in the Forms repository on the DCYF intranet)

Resources

DCYF Administrative 12.04 Acceptable Use of Technology Resources and the Internet policy (located on the Administrative Policies page on the DCYF intranet)
OCIO Policy 121 - IT Investments - Approval and Oversight Policy