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: December 1, 2021
Sunset Review Date: December 31, 2025
Approved by: Frank Ordway, Chief of Staff

Purpose

The purpose of this policy is to provide guidance on protecting confidential information that is collected, used, maintained, or disclosed by Department of Children, Youth, and Families (DCYF).

DCYF is not a Health Insurance Portability and Accountability Act (HIPAA)-covered entity.

Scope

This policy applies to DCYF employees, volunteers, interns, and work study students. For represented employees, the collective bargaining agreements will prevail if this policy is determined to be in conflict.

Laws

Chapter 13.50 RCW	Keeping and Release of Records by Juvenile Justice or Care Agencies
RCW 26.44.031	Records-Maintenance and disclosure-Destruction of screened-out, unfounded, or inconclusive reports-Rules-Proceedings for enforcement
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 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]
RCW 43.17.410	Sensitive personal information of in-home caregivers for vulnerable populations-Release of information prohibited
RCW 43.17.425	Immigration and citizenship status-State agency restrictions
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

Executive Order 17-01	Reaffirming Washington's Commitment to Tolerance, Diversity, and Inclusiveness
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 (HIPAA) of 1996

Policy

1. DCYF must:
    a. Not collect, use, or disclose confidential information, e.g., social security numbers (SSNs) or other sensitive personal and financial identifying numbers, unless:
        i. It is either:
            A. Required by law.
            B. 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, or e-mail.
    b. Prominently display:
        i. This policy on the DCYF website home page and on any other page where personal information is collected or viewable.
        ii. The security and privacy notice on DCYF internet public-facing websites and web applications to inform users of the collection, use, and security of their personal information when accessing DCYF websites or web applications.
    c. Not require clients to waive their right to file a privacy complaint as a condition of eligibility for services and benefits.
    d. For:
        i. Biometric identifiers:
            A. Inform and obtain consent from clients, employees, volunteers, interns, work study students, contractors, and vendors prior to collecting or using their biometric identifiers, unless authorized under RCW 40.26.020. The consent must:
                I. Clearly state the purpose and use of the biometric identifier.
                II. Be retained for the duration of the retention of the biometric identifier.
            B. Only use the biometric identifiers as permitted by the terms of the notice and consent. Biometric identifiers must:
                I. Not be sold or given away.
                II. Not be retained longer than needed to accomplish the purpose for collection.
                III. Only be disclosed as outlined in chapter 42.56 RCW.
                IV. Only be stored or transmitted as outlined in the OCIO security standards and DCYF Administrative 12.04 Acceptable Use of Technology Resources and the Internet policy.
        ii. Immigration and citizenship status:
            A. Only inquire about or request documents related to an individual's immigration or citizenship status when it is required by federal or state law

when the sole purpose of the inquiry or request is to identify compliance with federal civil immigration laws.

B. Not use immigration or citizenship status or place of birth information when registering crime victims or witnesses for the Victim Witness Notification Program.

C. Only provide or disclose personal information to individuals engaged, or intending to engage, in immigration enforcement without a court order or judicial warrant when required under chapter 42.56 RCW. This includes federal immigration authorities.

iii. FamLink and other applications containing Social Security Administration (SSA) information, perform random sampling and periodic reviews of user access and user activity.

2. The DCYF official SSA contact or designee must notify the SSA, if breaches or potential breaches contain SSA-provided information.
3. The chief information security officer (CISO) or designee must approve DCYF security notices.
4. The privacy officer must:
    a. Continually review and update this policy to align with current information collection and retention procedures.
    b. Approve DCYF privacy notices.
    c. For breaches or potential breaches of confidential information, notify:
        i. Individuals who may be affected as described in RCW 42.56.590.
        ii. The Office of the Attorney General (AGO) if a single breach requires notification to more than 500 individuals.
    d. Investigate and resolve complaints related to possible privacy violations.
5. Supervisors must verify their direct reports who are:
    a. Paid employees, interns, or work study students complete the:
        i. Nondisclosure of Confidential Information DCYF 03-374F form on their start date and annually thereafter.
        ii. Security training within the timeframes outlined in the Mandatory Training Manual.
    b. Unpaid volunteers, interns, or work study students complete the Agreement on Nondisclosure of Confidential Information-Non Employee DCYF 03-374B form prior to gaining access to confidential information.
6. Paid employees, interns, or work study students must:
    c. Complete the Nondisclosure of Confidential Information DCYF 03-374F form on their start date and annually thereafter.
    d. Complete the security training within the timeframes outlined in the Mandatory Training Manual.
7. Unpaid volunteers, interns, or work study students must complete the Agreement on Nondisclosure of Confidential Information-Non Employee DCYF 03-374B form prior to gaining access to confidential information.
8. Employees, volunteers, interns, and work study students must:
    a. Not intimidate, threaten, coerce, discriminate against, or take other retaliatory actions toward individuals filing a privacy complaint, per DCYF Administrative 11.03 Preventing and Addressing Discrimination, Harassment, Sexual Harassment policy.
    b. Safeguard personal information from inappropriate use and disclosure.
    c. Retain confidential information only as long as needed to carry out the purpose for which it was collected and according to the records retention schedule.
    d. Make reasonable efforts to limit the inclusion of personal information, including SSNs, in records.
    e. Dispose of records containing personal information, as outlined in DCYF Administrative 13.06 Establishing DCYF Records Management and Retention Procedures.

f. Adhere to the privacy principles and best practices established by the Office of Privacy and Data Protection.
g. Follow DCYF Administrative policies:
    i. 13.01 Use and Destruction of Health Care Information, if health care information is improperly disclosed or received.
    ii. 13.02 Management of the Litigation Discovery Process, if litigation is anticipated or a lawsuit or claim has been filed against DCYF.
    iii. 13.03 Response to Litigation-Related Documents, Contacts by Opposing Counsel, Providing Opposing Testimony, and Requesting Legal Representation, when responding to litigation-related documents and contacts by an attorney not employed or contracted by the AGO.
    iv. 13.05 Public Records Requests and Disclosure, when responding to public records requests.
h. Follow this policy. Failure to do so may result in disciplinary action, up to and including dismissal.

Procedures

Breach Notifications
When a breach or potential breach of confidential information is discovered:

1. Employees, volunteers, interns, and work study students must immediately notify the following by email, the:
    a. Privacy officer
    b. IT Security Office
2. When notified of a breach or potential breach, the:
    a. Privacy officer must:
        i. Track and coordinate written or electronic notification to individuals affected or potentially affected, per RCW 42.56.590 and RCW 70.02.290.
        ii. Notify the AGO within 30 calendar days of discovery, if it affects or potentially affects over 500 individuals.
    b. IT Security Office must follow internal IT procedures to identify content and corrective actions, when needed.
3. When the IT Security Office determines a breach or potential breach contains SSA-provided information:
    a. The CISO or designee must immediately notify the DCYF official SSA contact or designee responsible for the systems security designated in the Information Exchange Agreement (IEA).
    b. When the DCYF official SSA contact or designee is notified of the breach or potential breach by the CISO or designee, they must:
        i. Immediately notify the SSA Regional Office or the SSA systems security contact.
        ii. If they cannot make contact:
            A. Contact the SSA National Network Service Center at 1-877-697-4889.
            B. Select “Security and PII Reporting” from the options list.
            C. Report the security incident.
        iii. Maintain and update the IEA with the SSA and the SSA will provide updates to the Electronic Information Exchange Procedures, as appropriate.

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).

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 does need 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 and telecommunication 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).
    - 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.

Federal Immigration Authority means any officer, employee, or person otherwise paid by or acting as an agent of the United States department of homeland security including but not limited to its sub-agencies, immigration and customs enforcement and customs and border protection, and any present or future divisions thereof, charged with immigration enforcement.

HIPAA-Covered Entities are health care providers, health plans, or health care clearinghouses as defined under the Health Insurance Portability and Accountability Act (HIPAA) and must comply with HIPAA.

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.

Protected Health Information (PHI), or HIPAA data, is any personal health information that can potentially identify an individual, that was created, used, or disclosed in the course of providing healthcare services, whether it was a diagnosis or treatment. PHI can include:

- The past, present, or future physical health or condition of an individual.
- Healthcare services rendered to an individual.
- Past, present, or future payment for the healthcare services rendered to an individual, along with any identifiers outlined under Health Insurance Portability and Accountability Act (HIPAA).

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 Breach 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.

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

Resources

DCYF Administrative 11.03 Preventing and Addressing Discrimination, Harassment, Sexual Harassment policy (located on the Administrative Policies site of the DCYF intranet)
DCYF Administrative 12.04 Acceptable Use of Technology Resources and the Internet policy (located on the Administrative Policies site of the DCYF intranet)
DCYF Administrative 13.01 Use and Destruction of Health Care Information policy
DCYF Administrative 13.02 Management of the Litigation Discovery Process policy (located on the Administrative Policies site of the DCYF intranet)
DCYF Administrative 13.03 Response to Litigation-Related Documents, Contacts by Opposing Counsel, Providing Opposing Testimony, and Requesting Legal Representation policy (located on the Administrative Policies site of the DCYF intranet)
DCYF Administrative 13.05 Public Records Requests and Disclosure policy (located on the Administrative Policies site of the DCYF intranet)
DCYF Administrative 13.06 Establishing DCYF Records Management and Retention Procedures policy (located on the Administrative Policies site of the DCYF intranet)
Information Exchange Agreement (located in the Contracts Office)
OCIO Policy 121 - IT Investments - Approval and Oversight Policy
Victim Witness Notification Program
WA State Records Retention Schedules