



POLICY TITLE:	<i>Personal Identifiable Information</i>		
 	CHILD AND FAMILY SERVICES AGENCY		
Approved By:	Date Approved:	Original Effective Date:	Last Revision:
Brenda Donald	April 5, 2019	August 31, 2018	

I. AUTHORITY	<p>The protected information requirements of the applicable provisions of the National Institute of Standards and Technology (“NIST”) Special Publication 800-171 (Rev 1); HIPAA 164.306, 312, and 314, D.C. Official Code 4-1303.06 et al.; District Personnel Manual Chapter 16; District Personnel Instruction No. 16-18; the LaShawn A. v. Bowser Implementation and Exit Plan (December 17, 2010); and Policy 0003 of the D.C. Office of the Chief Technology Officer’s (OCTO) Information Security Program.</p>
II. APPLICABILITY	<p>This policy, as described, applies to Child and Family Services Agency (“CFSA”) and Private Agency workforce members, full and part-time employees, contractors, volunteers, and interns authorized to use CFSA equipment or facilities and provided with a user account to access CFSA resources. Applicable parties are referred to herein as “users”.</p>
III. RATIONALE	<p>The purpose of this policy is to ensure that anyone who collects or uses personal identifiable information (“PII”) at CFSA does so in compliance with state and federal regulations and best practices for information security. To provide permissible access, the CFSA Chief Information Security Officer (“CISO”), in collaboration with OCTO, controls individual access to FACES and any network resource and information systems owned or entrusted to CFSA.</p> <p>Having a policy ensures that users understand their responsibilities to protect data, including electronic protected health information (“ePHI”), that is stored in or transmitted through FACES or other Agency management information systems.</p>
IV. POLICY	<p>The CFSA Director adopts this policy to be consistent with the Agency’s mission and all applicable federal, District of Columbia laws, personnel regulations, and applicable collective bargaining agreements.</p> <p>This policy establishes responsibilities for managing privacy risk in creating, collecting, maintaining, using, storing, transmitting, protecting, and destroying PII (i.e., name, Social Security Number, biometric records, date and place of birth, mother’s maiden name). Management shall ensure that users understand their responsibilities to protect data, including electronic protected health information (“ePHI”) that is stored in or transmitted through FACES or other Agency management information systems.</p> <p>CFSA prohibits connecting personal devices to CFSA’s network and information systems or a personal mobile device or storage device.</p>

V. CONTENTS	A. National Institute of Standards and Technology B. Waiver of PII Requirements C. Access to FACES, CFSA, District of Columbia Resources, and Acceptable Use D. Monitoring Network Information
VI. SECTIONS	Section A: National Institute of Standards and Technology The National Institute of Standards and Technology (“NIST”) increases safety and use to prevent, detect, and respond to cyber-attacks. CFSA is to adhere to NIST standards to ensure safety, reliability, and environmental care. Standardization ensures that products, services, and methods are appropriate for their intended use. It ensures that products and systems are compatible and interoperable. CFSA abides the following NIST requirements: <ol style="list-style-type: none"> 1. Authority to Collect: The organization requires a signed contract to determine the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need. 2. Purpose Specification: The signed contract describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. 3. Governance and Privacy Program: CFSA shall: <ol style="list-style-type: none"> a. Appoint a designee accountable for developing, implementing, and maintaining an organization wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems. b. Monitor federal privacy laws and policy for changes that affect the privacy program. c. Allocate budgeting and staffing resources to implement and operate the organization-wide privacy program. d. Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures. e. Develop, disseminate, and implement operational privacy policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII. f. Update privacy plan, policies, and procedures, as required to address changing requirements biennially. g. For organizations external to CFSA, identify the designee for compliance with privacy requirements (e.g. ensuring that there is a senior privacy official and there are compliance officers). h. Establish and annually exercise incident reporting for breach incidents. 4. Privacy Impact and Risk Assessment: CFSA shall: <ol style="list-style-type: none"> a. Document and implement a risk management process that assesses privacy risk to individuals resulting from the collection, sharing,

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 2 of 9

	<p>storing, transmitting, use, and disposal of ePHI.</p> <p>b. Conduct privacy impact assessment (“PIA”) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, DC Privacy Policy, or any existing CFSA policies and procedures. This includes completing, submitting and having an approved PIA completed by the CISO.</p> <p>5. Privacy Requirements for Contractors and Service Providers: CFSA shall:</p> <p>a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers.</p> <p>b. Include privacy requirements in contracts and other acquisition-related documents. This includes, but is not limited to, having established privacy roles, responsibilities, and access requirements for contractors, service providers, and privacy requirements in all contracts and acquisition-related documents.</p> <p>c. CFSA shall monitor and audit privacy controls and internal privacy policy as required ensuring effective implementation.</p> <p>6. Privacy Awareness and Training: CFSA shall:</p> <p>a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.</p> <p>b. Administers targeted privacy training, role-based privacy training for personnel having responsibility for PII.</p> <p>c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.</p> <p>7. Privacy Reporting: CFSA shall develop, update, and disseminate reports to the Office of the DC Attorney General and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.</p> <p>8. Privacy-Enhanced System Design and Development: CFSA shall design information systems to support privacy by automating privacy controls thru defining and categorizing data sets.</p> <p>9. Accounting of Disclosures: CFSA shall keep an accurate accounting of disclosures of information held in each system of records under its control. CFSA shall retain the accounting of disclosures for the life of the record or a minimum of five years after the disclosure is made whichever is longer. CFSA shall make the accounting of disclosures available to the person names in the record upon said person’s request. Information contained in the accounting of disclosures includes:</p> <p>a. Date, nature, and purpose of each disclosure of a record.</p> <p>b. Name and address of the person or agency to which the disclosure was made.</p> <p>10. Data Quality: CFSA shall:</p> <p>a. Confirm to the greatest extent practicable upon collection or creation</p>
--	--

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 3 of 9

of PII, the accuracy, relevance, timeliness, and completeness of that information.

- b. Collect PII directly from the individual to the greatest extent practicable.
- c. Ensure that the initial input of PII automatically corrects through the system.
- d. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.
- e. Request that the individual or individual's authorized representative *validate PII* during the collection process.
- f. Request annually that the individual or the individual's authorized representative *revalidates that the PII* collected is still accurate.

11. Data Integrity and Data Integrity Board: CFSA shall:

- a. Document processes to ensure the integrity of PII through existing security controls.
- b. Establish a Data Quality & Integrity Board when appropriate to oversee organizational Computer Matching Agreements (i.e., matches public record or data collected by another DC Agency) and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

12. Minimization of PII: CFSA shall:

- a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.
- b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.
- c. Conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings quarterly to ensure that only PII identified in the notice is collected, retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
- d. Where feasible and within the limits of technology, locate, remove, redact specified PII, and use anonymization (i.e., the process of either encrypting or removing) and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

13. Data Retention and Disposal: CFSA shall:

- a. Retain each collection of PII for no less than seven years to fulfill the purpose(s) identified in the notice or as required by District law.
- b. Dispose of, destroy, erase, and anonymize the PII, regardless of the method of storage, in accordance with a National Archive and Records Administration-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.
- c. Use compliant deletion software to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

POLICY TITLE

Personal Identifiable Information

PAGE NUMBER

Page 4 of 9

- d. Configure, where feasible, its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

14. Minimization of PII Used in Testing, Training, and Research: CFSA shall:

- a. Develop procedures that minimize the use of PII for testing, training, and research.
- b. Implement controls to protect PII used for testing, training, and research.
- c. Use, where feasible, techniques to minimize the risk to privacy of using PII for research, testing, or training such as de-identification.

15. Consent: CFSA shall:

- a. Provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection
- b. Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII
- c. Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII
- d. Ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

16. Individual Access: CFSA shall:

- a. Provide individuals the ability to have access to their PII maintained in its system(s) of records.
- b. Publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records.
- c. Publish access procedures in System of Records Notices (“SORNs”).
- d. Adhere to Privacy Act requirements and guidance for the proper processing of Privacy Act requests.

17. Redress: CFSA shall:

- a. Provide a process for individuals to have inaccurate PII maintained by CFSA corrected or amended, as appropriate.
- b. Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended.

18. Complaint Management: CFSA shall implement a process for receiving and responding to complaints, concerns, or questions about CFSA’s privacy practices through the CFSA helpdesk and ticketing tracking system.

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 5 of 9

	<p>19. Inventory of PII: CFSA shall:</p> <ul style="list-style-type: none"> a. Establish, maintain, and update annually an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. b. Provide each update of the PII inventory to the Chief Information Officer or CISO annually to support the establishment of information security requirements for all new or modified information systems containing PII. <p>20. Privacy Incident Response: CFSA shall:</p> <ul style="list-style-type: none"> a. Develop and implement an Incident Response Policy to include PII security. b. Provide an organized and effective response to privacy incidents in accordance with CFSA’s Incident Response Policy. <p>21. Privacy Notice: CFSA shall:</p> <ul style="list-style-type: none"> a. Provide effective notice to the public and to individuals regarding: <ul style="list-style-type: none"> i. Its activities that impact privacy, collection, use, sharing, safeguarding, maintenance, and disposal of PII. ii. Authority for collecting PII. iii. Choices, if any, that individual may have regarding how CFSA uses PII and the consequences of exercising or not exercising those choices. iv. The ability to access and have PII amended or corrected if necessary. b. Describe: <ul style="list-style-type: none"> i. The PII CFSA collects and the purpose(s) for which it collects that information. ii. How CFSA uses PII internally. iii. Whether CFSA shares PII with external entities, the categories of those entities, and the purposes for such sharing. iv. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent. v. How individuals may obtain access to PII. vi. How the PII will be protected. c. Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change. <p>22. System of Records Notice and Privacy Act Statements: CFSA shall:</p> <ul style="list-style-type: none"> a. Publish SORNs in the District of Columbia Register, subject to required oversight processes, for systems containing PII. b. Keep SORNs current.
--	---

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 6 of 9

	<p>a. Include Privacy Act Statements on its forms used for collecting PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.</p> <p>23. Dissemination of Privacy Program Information: CFSA shall:</p> <p>a. Ensure that the public has access to information about CFSA’s privacy activities and is able to communicate with its Senior Agency Official and Chief Privacy Officer about privacy.</p> <p>b. Ensure that CFSA’s privacy practices are publicly available through CFSA’s website.</p> <p>24. Internal Use: CFSA shall uses PII internally only for authorized purposes.</p> <p>25. Information Sharing with Third Parties: CFSA shall:</p> <p>a. Share PII externally, only for authorized purposes in accordance with the Privacy Act or other applicable laws.</p> <p>b. Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.</p> <p>c. Monitor, audit, and train CFSA staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.</p> <p>d. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.</p> <p>e. Keep a current record of authorized persons who may access PII from a client’s file.</p> <p>f. Ensure that persons claiming to be governmental employees provide proof of government status, such as a legitimate government e-mail extension (e.g. xxx.gov).</p> <p>g. Obtain proof of the requestor’s identity for every external request for information. Identity shall be confirmed by obtaining a copy of the requestor’s driver license or another form of government issued identification.</p> <p>h. Ensure that documentation required for certain uses and disclosures of information may be provided in electronic form, such as scanned images or pdf files.</p> <p>i. Ensure that documentation requiring signatures may be provided as a scanned image of the signed document or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.</p>
	<p>Section B: Waiver of PII Requirements</p> <p>1. In the event that compliance with this policy is not possible or practical, the System Owner shall apply for a waiver of one or more requirements</p>

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 7 of 9

	<p>of this policy. The waiver request shall be fully justified and supported by the CFSA CISO. Waivers may be in memorandum format, and shall:</p> <ol style="list-style-type: none"> a. Cite the specific mandatory practice(s) for which the waiver is requested. b. Explain the rationale for the requested waiver. c. Describe compensating controls to be in place during the period of the requested waiver until systems are compliant with this policy. d. Provide an action plan, with target dates, for compliance. <ol style="list-style-type: none"> 2. The CFSA's CISO or designee shall review waiver requests and forward them to the CFSA Change Control Board ("CCB") for a final decision. The CCB shall render a decision within 30 calendar days of receipt. If CCB has not rendered a decision within 30 calendar days, then the CISO or designee shall notify the originating CFSA office. The lack of a response within 30 calendar days is not an approval or denial of the waiver request. 3. The decision letter shall either: <ol style="list-style-type: none"> a. Approve the waiver and state all of the conditions, if any, for operating the information system under the waiver, including any waiver expiration date; b. Deny the waiver and state the basis for the denial; or, c. Request any additional information needed to make a decision on the waiver request. 4. Approved waivers shall document all of the conditions as part of the System Security Plan (SSP) for operating the information system under the waiver. Identical systems under the same management authority and covered by one SSP require only one waiver request.
	<p>Section C: Access to FACES, CFSA, District of Columbia Resources, and Acceptable Use</p> <ol style="list-style-type: none"> 1. To grant a user access to FACES security system and a user account, a user must complete FACES training. Training is required to facilitate an understanding of required acceptable usage of these resources to establish the various accounts and sharing of information to include but not limited to FACES and ePHI. 2. Users shall complete the appropriate security forms as required by the CFSA's Child Information Systems Administration (CISA).
	<p>Section D: Monitoring Network Information</p> <ol style="list-style-type: none"> 1. All private electronic mail messages sent or received over CFSA networks shall be subject to monitoring. If CFSA's CISA has reasonable cause to suspect illegal or illicit activities, then CISA and the OCTO Security Group reserves the right to inspect all network activities without notice, consent or a search warrant. 2. CFSA shall assume NO obligation to inform the user that, if required by law, it has disclosed information transmitted over its network to protect

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 8 of 9

	<p>CFSA and others from harm or to ensure proper operation of the system.</p> <ol style="list-style-type: none">3. The CISO shall inform users that the Agency shall only disclose information in order to comply with a court order, subpoena, summons, discovery request, warrant, statute, regulation, or governmental request.4. Violators of this policy or applicable law shall be subject to disciplinary action up to and including termination of employment, as well as possible legal action.
--	--

POLICY TITLE	PAGE NUMBER
Personal Identifiable Information	Page 9 of 9