STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, June 26, 2023

CF OPERATING PROCEDURE
NO. 50-26

Systems Management

POLICY ON AGREEMENTS INVOLVING DATA SHARING

Table of Contents

1. Purpose. This operating procedure establishes policy to govern the development and maintenance of Department Data Sharing Agreements as they are designed to effectively cover digital data sharing. A Data Sharing Agreement (DSA) is an agreement between a discloser of data and recipient(s) of data engaged in collaboration and development. Recipients of Department data are typically external partners seeking data to conduct academic research, scientific research or stakeholders seeking to conduct business with the State of Florida. As a discloser and a recipient of data, the Department of Children and Families (Department or DCF) often seeks to share data with universities, other government agencies, private entities and other external partners in furtherance of the Department's mission, vision, and values.

2. Scope. This operating procedure applies to all Department employees and contractors.

3. Authority.

a. Chapter 60GG-2, Florida Administrative Code (F.A.C.), "Florida Cybersecurity Standards".

b. Section 20.05, Florida Statutes (F.S.), "Heads of departments; powers and duties".

c. Section 20.19, F.S., "Department of Children and Families".

d. Section 282.318, F.S., "State Cybersecurity Act".

e. 45 CFR Parts 160 and 164, Subparts A and C, Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules.

f. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, "Security and Privacy Controls for Information Systems and Organizations".

g. Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 Requirements.

h. 5 U.S.C. 552a, Privacy Act of 1974 - Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration Technical System Security Requirements (TSSR), v.10.4.

i. Internal Revenue Service, Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Rev. 11-2021.

j. CFOP 5-2, "Departmental Administrative Publications System."

4. Definitions. For the purposes of this operating procedure, the following terms shall be understood to mean:

a. Agreement. In the context of this operating procedure, an agreement is a formal document, signed by appropriate authority from each party involved, which includes, but is not limited to, the criteria for access to data, conditions of data use, retention of data periods, and the duration and effective date of the agreement. This type of sharing agreement can be in the form of a service level agreement, memorandum of understanding, memorandum of agreement, interagency agreement, cooperative agreement, or a data sharing or data matching agreement.

b. Agreement Coordinator. The representative of the DCF program office that initiates and drives a DSA internal to DCF. This role is responsible for circulating a DSA proposed by their program office for development and then through appropriate interoffice review process for final approval. The Agreement Coordinator will also ensure a draft DSA is distributed to their external partner(s) for internal review and feedback. The contact information for the Department's Agreement Coordinator and the external partner's Agreement Coordinator must be provided within the body of the DSA so that there is at least one Agreement Coordinator listed for each participating agency or external partner.

c. Chief Information Officer (CIO). The duties of the Chief Information Officer (CIO) include the management and oversight of strategy and implementation for the usability of information technology and the business systems that support enterprise goals.

d. Confidential Information. Information that is exempted from disclosure requirements under the provisions of applicable state and federal law, e.g., section 119.07, F.S., "Public Records."

e. Data Owner. At DCF the Secretary of the Department is ultimately responsible for the collection, maintenance, and dissemination of Department data. The Secretary is also the overall mission and business owner for the Department, providing the broad expression of DCF business goals and the specified target outcomes for all DCF business operations.

f. Data Sharing. The transfer of digital data, between two or more parties, which may be unidirectional or bidirectional in nature. DCF may disclose its Departmental data, be the recipient of data owned by another party, or act as an intermediary in transferring data from one entity to another.

g. Director of Enterprise Data Management. The Director of the Enterprise Data Management (EDM) team facilitates cross-departmental data sharing and assists Department data-sharing initiatives among many external entities, in addition to providing expertise and collaboration in the area of data intelligence, analytics, and reporting.

h. Employee. Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. Also, for the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff who have access to Department information technology resources, including contracted staff and contracted vendor staff.

i. External Partners. The colleges, universities, other government agencies, private entities and community partners and community stakeholders that the Department seeks to productively share data with across the state of Florida and beyond in furtherance of the Department's mission, vision, and values.

j. Federal Tax Information (FTI). A term for data that consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections and safeguarding requirements including IRS oversight. FTI is categorized as sensitive and may contain personally identifiable information (PII).

k. Information and Data Custodians. Individuals or groups at DCF that ensure the careful and responsible management of information and data belonging to the Department as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information and data custodians act a stewards, providing maximum access to information and data elements, balancing this work with the shared obligation to protect the information in accordance with the

provisions of law and any associated security-related state or federal policies, directives, regulations, standards, and guidance.

l. Information Owner. Under the direction of the Secretary, the Director of the program office ultimately responsible for the collection, maintenance, and dissemination of a specific collection of program office information or a program area business information system.

m. Information Security Manager. The DCF Information Security Manager (ISM) is the person designated by the Secretary of the Department to administer the Department's information technology security program and serve as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with §282.318, Florida Statutes, and Chapter 60GG-2, F.A.C.

n. Memorandum and Agreement Collection. The DCF-MAC (Memorandum and Agreement Collection) is the Department's searchable repository for all Department agreements. In this system, Digital Forms are enabled to allow all DCF agreement coordinators and contract managers to submit and update agreements and applicable contracts into the system. The DCF-MAC indexing system will provide efficiency in locating, monitored, and maintaining agreements in a centralized location. Additionally, the development of the MAC is another way in which the Department is championing the state's interoperability goals.

o. DCF-MAC is a powerful tool to improve your office's organization and efficiency. All Contracts and Agreements in the Department should be entered into the DCF-MAC System, creating an easily accessed archive of all files for future reference and renewals.

p. OITS Data Agreement Coordinator. This role is not the same as the Agreement Coordinator for the respective program office or external partner but does work in partnership with those two roles. This role is from within the Office of Information Technology Services (OITS) that is responsible for maintaining completed or renewed DSAs in the Department's DCF-MAC (Memorandum and Agreement Collection) indexing system. The archived DSA records in the DCF-MAC can then be retrieved for reference and review by Department staff. The contact information for the OITS Data Agreement Coordinator is provided within the body of the DSA template, CF 122. The Agreement Coordinators from the respective DCF program offices are responsible for working with the OITS Data Agreement Coordinator to ensure copies of the final approved and signed DSA are placed in the DCF-MAC indexing system.

q. Personal Identifying Information (PII). Any information about an individual maintained by a department or agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This information is sensitive and confidential.

r. Personal Information (PI). Any recorded information about an identifiable individual that may include name, address, email address, phone number, race, nationality, ethnicity, origin, skin color, religious or political beliefs or associations, age, sex, sexual orientation, marital status, family status, identifying numbers, codes, symbols, fingerprints, blood type, inherited characteristics, health care history including information on physical/mental disability, educational, financial, criminal, employment history, and personal views.

s. Protected health information (PHI). Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

t. System Owner. Program office having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

5. Guiding Principles. DCF is committed to the goal of ensuring appropriate data handling processes to further protect the integrity, security, and confidentiality of Department data. To help ensure that DCF can continuously meet this goal, any data shared by the Department, whether received from or disclosed to another entity, will be protected by a comprehensive written agreement that accurately describes the mechanics of the agreed-upon data sharing venture.

a. The DCF Office of Information Technology Services (OITS) actively reviews any data sharing agreements under consideration by DCF to verify appropriate data quality and security measures are in place. Within OITS the DCF ISM reviews DSAs to ensure all applicable and appropriate security controls and state and federal audit compliance controls have been effectively addressed. The EDM team in OITS reviews DSAs for content and quality control to further facilitate quality data sharing across the state of Florida. Only after these two separate quality reviews do DSAs go to the CIO for review and approval.

b. Special Note. Any would-be data recipient(s) requesting federally supplied social security data in the custody of DCF must be approved by the U. S. Social Security Administration (SSA) to receive specified SSA data prior to receiving any such data through a DSA with DCF. Any DSA DCF enters into with any recipient entity / entities who have received the required SSA approval to have access to SSA data in DCF's custody shall be required in the body of the actual Data Sharing Agreement to notify the DCF ISM and DCF CIO within one (1) hour of any detected potential breach of SSA data. The same is true of Internal Revenue Service (IRS) data entrusted to the custody of DCF; prior approval of the IRS must be obtained, and it shall be required in the body of the actual DSA that the DCF ISM and DCF CIO are to be notified within one (1) hour of any detected potential breach of IRS data.

6. Procedures for DCF Data Sharing Agreement Proposals. In addition to the procedural steps outlined below, DCF employees will follow any and all other authorized DCF policies and procedures developed to better facilitate agency data sharing:

a. Legal Consultation. When a DCF program office identifies a possible opportunity for the Department and or the State of Florida to benefit from the creation and maintenance of a DSA, the respective DCF program office should first confirm with the DCF Office of General Counsel (OGC) that the data their program office owns, and which is under discussion to be shared can be lawfully shared by the Department. Once that confirmation has been received, the respective DCF program office should follow any OGC guidance provided on how best to share the data in a manner consistent with Federal and State law.

b. Begin Draft Template. After conferring with Office of General Counsel, the respective DCF program office staff opting to propose a DSA should obtain a Data Sharing Agreement template (form CF 122, available in the DCF Forms) and complete a draft template.

c. Draft Circulation. The DCF program office staff will either use the Department approved document routing system (Document Production System, DPS), as per CFOP 5-2, “Departmental Administrative Publications System,” or Department email to circulate a copy of their draft through a formal internal review process for both the Draft Review Phase and the Review for Signature Phase.

d. Draft Review Phase. The draft DSA should be reviewed by these teams as appropriate to resolve any identified issues before moving on to the Review for Signature Phase.

(1) Internal Review. The internal review team for constructing draft Data Sharing Agreements at DCF must include, but is not limited to:

(a) Appropriate Program Office Management.

(b) Legal Review by OGC.

(c) OITS (Director of Enterprise Data Management's team, DCF ISM, etc.); and,

(2) External Review. The Department includes external partner(s) which the department share data with as a recipient or provider in the DSA review process. The DCF program office's Agreement Coordinator is responsible for coordinating the review of the draft DSA by the External Partner(s).

e. Review for Signature Phase.

(1) OGC and Program Office. Once the draft DSA has been agreed upon by the External Partner(s), the DCF program office's Agreement Coordinator will then send their Final Draft through the Review for Signature phase. The Final Draft should be reviewed and approved first by OGC, before proceeding on to the DCF program office's head or Designee for their signature on the DSA.

(2) OITS and CIO. Next, the Final Draft moves to OITS where it should be reviewed and approved first by the DCF ISM, then by the Director of Enterprise Data Management, before moving on to the DCF CIO for their review and signature.

Once the CIO has signed the DSA, the hardcopy should go to the IT Data Agreement Coordinator to be scanned into electronic format and entered into the DCF-MAC indexing system. Data specifications inventory shall include storage locations, exchange time, and record details.

Upon completion the signed and approved DSA should go back the DCF Agreement Coordinator. The DCF Agreement Coordinator will ensure that a final signed copy gets added to the DCF-MAC indexing system and, if the Document Production System (DPS) was used, be responsible for coordinating the closing of the DPS Document ID Number.

7. Existing DSAs. Changes, renewals, modifications, or other alterations to existing DCF Data Sharing Agreements should follow the same internal review processes.

8. Procedures for Internal to OITS DSA Maintenance and Review. OITS is responsible for documenting in a Standard Operating Procedure (SOP) any OITS processes and procedures associated with OITS review and maintenance of signed DCF Data Sharing Agreements within the DCF-MAC indexing system.

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL
June 26, 2023: Annual review and revision completed; section *Procedures for DCF Data Sharing Agreement Proposals* updated with the current Department's document routing system, Document Production System (DPS). This operating procedure supersedes CFOP 50-26, dated April 6, 2022.