Records Confidentiality/Retention/Requests

PURPOSE

To provide guidance to Early Learning Coalitions (ELCs, coalitions), the Office of Early Learning (OEL, the Office) employees, other OEL subrecipients and other early education program partners regarding what information is confidential by law, timeframes for records retention, and how to process records requests and subpoenas.

AUTHORITY

- Chapter 119, F.S., Public Records
- Section 1002.72, F.S., Records of Children in the Voluntary Prekindergarten Education Program
- Section 1002.97, F.S., Records of Children in the School Readiness Program
- Section 1002.221, F.S., K-12 Education Records; Public Records Exemption
- 45 C.F.R. Pt. 5b, Privacy Act Regulations
- 20 U.S.C. § 1232g, Family Educational and Privacy Rights
- 2 CFR Part 200.79, Personally Identifiable Information (PII)
- 2 CFR Part 200.82, Protected Personally Identifiable Information (Protected PII)
- 2 CFR Part 200.303(e), Internal controls to safeguard PII and PPII
- 2 CFR Part 200.335, Methods for collection, transmission and storage of information
- 2 CFR Part 200.337, Restrictions on public access to records
- Chapter 815, F.S., Computer-Related Crimes
- Section 501.171, F.S., Security of confidential personal information (aka the Florida Information Protection Act of 2014 (FIPA))

Definitions and Abbreviations

Breach

Defined in Chapter 282.0041, F.S., means a confirmed event that compromises the confidentiality, integrity, or availability of information or data.

Breach of Security

Defined in Chapter 501.171, F.S., as the unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Confidential

As used in this guidance, the term "confidential" refers to entire record systems, specific records or individually identifiable data that by law are not subject to public disclosure under Article I, Section 24 of the Florida Constitution and Chapter 119, Public Records, of the Florida Statutes. When applicable, confidentiality covers all documents, papers, computer files, letters and all other notations of records or data that are designed by law as confidential. Further, the term confidential also covers the verbal conveyance of data or information that is confidential.

These confidential records may include but not be limited to, social security numbers, parent and child information, payments, childcare providers, household demographics and resource and referrals.

Confidentiality

The state of keeping or being kept secret or private.

Florida Information Protection Act of 2014 (FIPA)

Statutory requirements that describe legal duties and responsibilities for covered entities to take reasonable measures to protect and secure electronic data containing customers' personal information. These requirements apply to any commercial or government entities operating in Florida (aka, third party agents, including ELCs and other OEL subrecipients). [Section 501.171, F.S.]

Information Technology Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information and technology resources. [Section 282.0041(14), F.S.]

Mobile Computing Device (aka portable storage media or peripheral devices)

A laptop or other portable device that can store, playback or process data via ports or wireless networking technology. Other covered media devices include hard drives, thumb drives, flash drives, tablets, cell phones, smart phones, wearable computing devices diskettes, CDs, etc. Such devices shall not be used to store any confidential data as described in this guidance.

Personally Identifiable Information (PII)

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, websites, and university listings. This type of information is considered Public PII and includes for example, first and last name, address, work telephone number, and general educational credentials.

The definition of PII is <u>not</u> anchored to any single category of information of technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. [2 CFR Part 200.79]

Protected Personally Identifiable Information (Protected PII or PPII)

Protected PII means an individual's first name or first initial and last name in combination with any one

or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial record and education transcripts. This definition does not include PII that is required by law to be disclosed. [2 CFR Part 200.82]

Public Agency

A state, county, district, authority, or municipal officer, or department, division, board, bureau, commission, or other separate unit of government created or established by law... and any other public or private person, partnership, corporation, or business entity acting on behalf of any public agency. [Section 119.011 (2), F.S.]

Public Records

All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material regardless of physical form, characteristics or means of transmission made or received in accordance with law or in connection with the official business of an agency. This definition includes communications made on personal cell phones/smart phones and other mobile devices, Facebook posts or other social media transmissions when such communications are made in connection with or relate to an entity's business operations. [Section 119.011 (12), F.S.]

Security Incident

Defined in Chapter 282.0041, F.S., means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

School Readiness (SR)

The School Readiness Program as established in Part VI of Chapter 1002, F.S., and authorized pursuant to the Child Care and Development Block Grant Trust Fund, 45 Code of Federal Regulations, parts 98 and 99.

Voluntary Prekindergarten (VPK)

The Voluntary Prekindergarten program, as established in Part V of Chapter 1002. F.S.

POLICY AND GENERAL PROCEDURES

This guidance applies to OEL, the ELCs and other OEL subrecipients. ELCs are responsible for requiring any subrecipients and subcontractors follow these guidance instructions and applicable grant award or contract terms and conditions. The collection, retention and production of public records are governed by the federal regulations and statutory authorities cited on the last page of this document.

Access

All records classified as public records must be open and available for inspection by any person unless otherwise specified by law. It is the responsibility of OEL, the ELCs, and other OEL subrecipients to maintain records in a location that is accessible to the public and in a manner (i.e., cost) that does not exceed the costs provided in Chapter 119, F.S., or as otherwise provided by law.

The rights of access as described in this guidance is not limited to the required retention period but is

in effect for as long as the described records are retained.

Disclosure Forms

Subrecipients and subcontractors are required to enter into and use appropriate nondisclosures agreements as necessary to maintain data confidentiality and security. Individuals who have access to such data are also required to complete an individual nondisclosure form that each ELC, other OEL subrecipient or subcontractor shall maintain on file.

Internal Controls

Each non-federal entity that administers or manages federally or state-funded grant programs must establish internal controls that provide reasonable assurance of compliance with federal statutes, regulations, and the terms and conditions of the Federal award.

Internal controls must specifically –

"Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state and local laws regarding privacy and obligations of confidentiality." [2 CFR Part 200.303(e), *Internal controls*]

Portable Devices – when to use them with confidential data

OEL, the ELCs, other OEL subrecipients (including any employees, subcontractors, agents or any other individuals exposed to confidential information) shall not store, or allow to be stored, any confidential information on any portable storage media or peripheral device with the capacity to hold information without encryption software installed on the devices meeting the standards prescribed in the National Institute of Standards and Technology Special Publication 800-111 (http://csrc.nist.gov/publications/PubsSPs.html#SP/800). Failure to strictly comply with this provision shall constitute a breach of this agreement's terms.

Records Custodian Contact Information

Each agency/entity shall have designated records custodian personnel. These are staff members who have it within their assigned duties to be responsible for responding to public records requests and to release or commuicate public records. Contact information for each entity's records custodian should be posted in the public/common area of the entity's administrative offices and on the entity's website.

A custodian of public records may designate another agency officer or employee to permit the inspection and copying of public records, but must disclose the identity of the designee to the person(s) requesting to inspect or copy public records.

The Public Records Custodian duties include (1) ensuring compliance with the Office's (or the ELC's) records management policies, standards and procedures, (2) provide training and technical assistance to staff as needed, (3) track and fill all public records requests, (4) communicate applicable citations for records not provided due to federal or statutory exemptions, (5) collect any fee in place for copying requested files, and (6) coordinate with other agency staff to ensure records retention rules and safeguarding procedures are in place and followed.

Security Incidents

The ELC and other OEL subrecipients agree to comply with s. 501.171, F.S., related to the security of confidential personal information and understand that for this purpose each entity will be considered a third party agent as referenced in this statutory section.

The ELC and other subrecipients shall immediately notify the Office's Information Security Manager and Inspector General of any Security Incident or Breach of Security of which it becomes aware by its employees, subcontractors, agents or representatives. Notwithstanding requirements of s. 501.171(3), F.S., within 24 hours of the incident the ELC shall provide written notification to the Office's Information Security Manager and Inspector General that identifies: (i) the nature of the unauthorized use or disclosure, (ii) the confidential information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what the ELC has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action the ELC has taken or shall take to prevent future similar unauthorized use or disclosure. The ELC shall provide any additional information, including a full written report, as reasonably requested by the Office.

Additional related instructions are included in the Florida Information Protection Act of 2014 (FIPA), Section 501.171, F.S.

- Written notice must be sent by third party agents to customers affected by the breach and must be sent to the Florida Department of Legal Affairs (DLA) within 10 days of discovery.
- See FIPA for specific information that must be provided in writing to DLA.
- If the breach is limited to encrypted data, the FIPA Safe Harbor provision applies and notice to customers/program participants is not required.
- Notice to credit reporting agencies is required for any breach affecting more than 1,000 individuals.
- Proper disposal methods for all customer personal information is described, regardless of the form of the data (paper or digital). Reasonable measures to dispose of customer information include "shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable by any means." s. 501.171(8). F.S.

CONFIDENTIAL RECORDS

VPK Records

Individual records of a child enrolled in the VPK program are confidential and exempt from disclosure under Section 1002.72, F.S. Records made confidential and exempt include the assessment data, health data, records of teacher observations and personal identifying information of an enrolled child and his or her parent or guardian. The exemption applies to records held by a coalition, OEL, or a VPK Education Program provider before, on or after the effective date of the exemption. A parent or guardian has the right to inspect, review and obtain a copy of the individual VPK Education Program record of his or her child. Pursuant to Section 1002.72(3), F.S., confidential and exempt VPK records may be released in limited circumstances.

SR Records

Individual records of children enrolled in SR programs, when held in the possession of SR providers, coalitions and OEL, are confidential and exempt from public disclosure. The child's parent or guardian

and other entities as set forth in the exemption are authorized to have access to the records, (Section 1002.97, F.S.).

Additional types of information that OEL and coalitions have access to, but are required to be confidential, include the following.

1. Section 402.308(3)(a), F.S. – OEL may only disclose social security numbers submitted by an applicant for a childcare facility license issued by the Department of Children and Families for child support enforcement purposes.
2. Section 409.175(16), F.S. – Specified personal information about foster care parents and their families that is contained in the licensing file of the Department of Children and Families is exempt from disclosure unless otherwise provided by Florida Statutes.
3. Section 409.821, F.S. – Information in an application for the determination of eligibility for the Florida Kidcare program that identifies applicants, including medical information and family financial information, is confidential and exempt from disclosure. In addition, any information obtained through quality assurance activities and patient satisfaction surveys that identify program participants, obtained by the Florida Kidcare program under cited statutes, is also confidential and exempt from disclosure.

Demographic Data in SR and VPK Programs

Demographic data (race/ethnicity, sex, age and, where known, disability status) for current and former applicants, clients on the Wait List, participating families and childcare providers must be stored in a manner that ensures confidentiality. The data shall be used only for the purposes of record keeping and reporting, determining eligibility in a nondiscriminatory manner or other use authorized by law. The data shall be used for statistical purposes only and not in any manner, that reveals the identity of the individual.

Medical Records & Disability – Related Information

Medical records and disability-related information on custodian and child records must be stored in a manner that ensures confidentiality, and only use the records for the purposes of record keeping and reporting and determining eligibility, or other use authorized by law.

Medical records and disability-related information must be maintained in the custodian's or child's file, stored in a secure area, and treated as confidential medical records. Access to disability-related or medical information shall be limited to the following:

1. To inform supervisors and managers regarding restrictions on the work or duties of an employee or participant and regarding necessary accommodations;
2. To inform first aid and safety personnel, when appropriate, if the disability might require emergency treatment or evacuation; and
3. To provide information, on request, to government officials investigating compliance with Federal law.

Social Security Numbers

Social security numbers are confidential pursuant to Section 119.071(5)(a), F.S., (5 USCA 552a). Redact

(eliminate) social security numbers from all documents prior to delivery, except as specifically provided by law, including documents to be filed with the courts and personnel records. The Privacy Act of 1974 (Public Law 93-579) requires that individuals required to disclose their social security number be informed whether disclosure is mandatory or voluntary and provided with a statement of the purpose for the collection. Additionally, Florida law allows commercial entities access to social security numbers if there is a legitimate business purpose and entities submit a request in writing. OEL shall maintain these requests for reporting purposes to the Florida Legislature. For commercial entity requests, please contact OEL's General Counsel.

PROCESSING RECORDS REQUESTS

Upon receipt of a public records request, the records custodian must determine the type of record requested, the location of the record and the legal requirements for disclosure of each record, including confidentiality and redaction, if necessary.

For requests submitted to the Office, coordination and notification to the OEL General Counsel and Public Information Officer is also required upon receipt of the request.

For requests submitted to an ELC or an OEL subrecipient, notification should be made in accordance with the entity's internal policies.

Confidential information that OEL receives from another agency retains its confidentiality unless otherwise provided by law. The requirements of the program that provides the information must apply.

Confidential and exempt records may be released to specified parties when authorized by law. The receiving party must protect the records in a manner that does not allow identification of an enrolled child, the child's parent or the child's legal guardian to persons not authorized to receive the records. If an exempt record is requested, an entity must state the basis for its refusal to release the requested exempt record.

Requests for public records may be submitted in person, by phone, electronically, in writing, or by contacting the OEL (or an ELC's) Custodian of public records and each records request should describe the specific items being requested. ELCs and other OEL subrecipients must respond in a timely fashion to all public records requests and may not (1) require requests be submitted in writing or (2) require the requestor to be physically present to inspect requested records. Public records policies should include a description of public records, record exemptions and general information on records access, inspection, examination and duplication processes (i.e., any fees charged for copies).

OEL, ELCs and other OEL subrecipients are only required to provide records that each entity regularly maintains. Entities are not required to generate new forms or records if the requested information is not already part of records made or received as part of its operations.

Requestors may be charged a nominal copying fee for the requested records. Additional fees may also apply and can be charged based on the actual cost incurred if the nature and volume of the recods requested require extensive use of IT resources and/or extensive clerical or supervisory assistance.

If the contractor has questions regarding the application of Chapter 119, Florida Statutes, or the contractor's duty to provide public records relating to this PO/contract, contact the custodian of public records at –

Office of Early Learning
250 Marriott Drive
Tallahassee, FL 32399
850-717-8550
PublicRecordsCustodian@oel.myflorida.com

RECORDS RETENTION

All records must be maintained for five (5) years from the date of the last reimbursement request for that fiscal year or until the resolution of any audit findings or any litigation related to the grant/contract, whichever occurs last. OEL, ELCs and other OEL subrecipients shall comply with the records retention requirements in Florida. The General Records Schedule GS1-SL for State and Local Government Agencies is located at www.dos.myflorida.com/library-archives/records-management/general-records-schedules.

Records retention schedules apply to records regardless of their physical format. Therefore, records created or maintained in electronic format must be retained in accordance with the minimum retention requirements, whether the electronic records are the record copy or duplicates. Whenever practicable, information should be collected, transmitted or stored in open and machine-readable formats.

Public records shall be maintained and preserved as follows:

(a) All public records should be kept in the buildings in which they are ordinarily used.
(b) Insofar as practicable, a custodian of public records of vital, permanent, or archival records shall keep them in fireproof and waterproof safes, vaults, or rooms fitted with noncombustible materials and in such arrangement as to be easily accessible for convenient use.
(c) Record books should be copied or repaired, renovated, or rebound if worn, mutilated, damaged, or difficult to read.

SUPPORT DOCUMENTATION

ELCs and other OEL subrecipients must establish prolicies that address proper records maintenance, retention and treatment of confidential records based on the Grant Agreement between OEL and the entity.

SUBPOENAS AND PUBLIC RECORDS REQUESTS

The Office of General Counsel is responsible for the acceptance of service of all subpoenas and public records requests that are directed to OEL. Each ELC or other OEL subrecipient shall designate the appropriate office or individual to accept service on behalf of the entity.

The mailing address and contact information for subpoenas and public records requests directed to OEL is –

The Office of General Counsel
Office of Early Learning
250 Marriott Drive
Tallahassee, FL 32399

Phone 850-717-8519
PublicRecordsCustodian@oel.myflorida.com

OTHER REQUESTS

Direct requests for **verification of employment** of the Office of Early Learning employees to –

Florida Department of Education
Human Resource Management
325 West Gaines Street
Tallahassee, Florida 32399
Phone 850-245-0505
Fax 850-245-9667

HISTORY

This program guidance replaces Florida's Office of Early Learning Fiscal Guidance 1.01. Issued July 1, 2015. Revised and reissued June 5, 2017; Effective July 1, 2017. Revised and Reissued July 1, 2019.

Please direct questions and comments to Office of Early Learning at 850-717-8500 or by email at oel.questions@oel.myflorida.com