Chapter 2 – Privacy and Security

Table of Contents

I. Document Revision History

Table 1. Document Revision History

Document Revision History				
Version Number	**Effective Date**	**Revision Date**	**Description**	**Author**
12.0	07/01/2017	05/10/2017	• Completed Version 12.0	SAMH Data Unit
12.0.1	07/01/2017	04/27/2018	• Updated CF114 – Security Agreement Form	Sarah Griffith
12.0.2	03/07/2018	06/05/2018	• Updated CF114 – Security Agreement Form March 2018	Sarah Griffith

II. Scope

This chapter provides general guidelines for ensuring the privacy and security of Protected Health Information (PHI) maintained in the Substance Abuse and Mental Health Data Information System (SAMHIS). The purpose of this chapter is twofold:

- To highlight the basic privacy and security safeguards that must be followed by authorized persons when performing a function that involves the use or disclosure of Protected Health Information in the SAMH system; and
- To describe the procedures for requesting and obtaining access to the SAMHIS system, including the policy directive for compliance with security awareness training requirements.

A copy of this chapter and appropriate form can be found on the Department web site at the following URL:

http://www.myflfamilies.com/service-programs/substance-abuse/pamphlet-155-2-v12

Pamphlet 155-2 chapters are listed and accessed individually.

III. Protected Health Information (PHI)

The SAMHIS system contains some of the 18 data elements contained in Title 45, Code of Federal Regulations (CFR), Parts 160 and 164, which is the Final Rule of the Health Insurance Portability and Accountability Act (HIPAA) establishing the national standards to protect individuals' medical records and other personal health information, including the privacy of individually identifiable health information. As such, only authorized persons, who must protect this individually identifiable information from accidental or intentional misuse, can access it.

The use or disclosure of any individually identifiable information in the SAMH system must be in accordance with all federal and state laws and regulations, including guidelines and standards to guard data integrity, confidentiality, availability, and reliability. Those that apply directly or indirectly to the security and privacy of data in the SAMH system include, but are not limited to, the following:

- Title 45 Code of Federal Regulations (CFR), Parts 160 and 164: Standards for Privacy of Individually Identifiable Health Information – Final Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Title 42 Code of Federal Regulations (CFR), Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records.
- Section 394.4615, Florida Statutes: Confidentiality of Mental Health Clinical Records.
- Section 397.501(7), Florida Statutes: Right to Confidentiality of Substance Abuse Client Records.
- Section 916.107(8), Florida Statutes: Confidentiality of Clinical Records for Mentally Deficient and Mentally Ill Defendants.
- Title 45 Code of Federal Regulations (CFRR), Part 142: Security and Electronic Signature Standards – Final Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Section 282.318, Florida Statutes: Security of Data and Information Technology.
- Department of Children and Families Operating Procedure (CFOP 50-2): Security of Data and Information Technology Resources.

IV. Basic Security Safeguards

Below are the minimum-security measures to protect data in the SAMH system from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside of the department.

1. Individual User Account: Each SAMH user must have a unique user account. This account should consist of the following information:

a. A personal identifier (i.e., User Logon ID) that is assigned and controlled by the DCF Security Officer in Tallahassee. To obtain this confidential User Logon ID, a user must complete, sign and submit the following four (4) documents to the appropriate Regional/Managing Entity Data Liaison or DCF Security Officer as outlined in IV.2:

i. The Database Access Request Form,
ii. The DCF Security Agreement Form (CF114),
iii. The online Security Awareness Training Certificate, and
iv. The online Health Insurance Portability and Accountability Act (HIPAA) Training Certificate.

Note: User requests for new or continued database access are scanned and maintained electronically by the SAMHIS Security Officer in Tallahassee.

b. A private password. The DCF Security Officer in Tallahassee will also assign a default password to each authorized SAMH user. The user will be prompted to change the default password immediately after logging into the system for the first time and regularly, thereafter, as required by the department.

2. The online Security Awareness Training and the HIPAA Training **must** be updated annually. In addition, all employees of the private and public agencies, who have access to departmental information shall comply with, and be provided a copy of CFOP 50-2, and shall sign the DCF Security Agreement form CF114 annually. Copies of the certificates and signed Security Agreement forms (CF114) should be kept in the Human Resources file of each employee. Managing Entities are responsible, by contract, for ensuring that all their appropriate staff members and staff members of their sub-contractors complete Form CF114 and take the updated trainings annually.

3. SAMH system users are prohibited from sharing their passwords and User Logon IDs with other individuals. They are also prohibited from sharing or discussing client-identifying information (PHI) with anyone unless the other person is also an authorized SAMH user or the agency has designated the person as having a need to know in accordance with agency operating procedures.

4. Any computer, which contains or has access to SAMH data or other individually identifiable information**, must** be password protected and should be located in a lockable room. The computer should be programmed to time out or to turn off automatically after 15 minutes or less without activity, and the room **must** be locked when the SAMH system user is not physically in the room.

5. Screensavers must be used and be password protected.

6. Any file containing confidential information that is not stored in a secure computer must be kept in a secure location whose accessibility requires the use of lock and key.

7. SAMH data or other individually identifiable information should never be sent to a fax machine number or to a printer unless a user is absolutely sure that the recipient equipment is located in a secure location accessible only to authorized users.

8. When sending client information by e-mail, it must be encrypted and password protected. A minimum of 128-byte encryption is required when using this process. Never send data being submitted in the body of the message. Passwords should be encrypted and sent in a separate email.

9. SAMH users at all levels (state, circuit/region and provider) should use preventive measures to minimize the risk of destruction, theft or loss of equipment and software, and to protect SAMH data from unauthorized disclosure, misuse, modification or destruction.

10. Supervisors and security SAMH Administrators at all levels (state, circuit/region and provider) are responsible for ensuring that SAMH users are trained and that appropriate access is allowed.

11. Security Parameters

Fail Logon Limit: 3 times
Password Expiration Days: 45 days
Password Minimum Length: 6 digits (numbers and/or letters)
Password Maximum Length: 8 digits (numbers and/or letters)
Previous Password Number: 15 (cannot use last 15 passwords)
Password Lock: 45 days of inactivity
Account Deactivation: 60 days of inactivity

12. An agency must: (1) immediately notify the Regional/Managing Entity Data Liaison or HQ SAMH Security Officer if a user has separated from the agency or no longer needs SAMHIS access in their current job duties, and (2) submit a completed Database Access Request Form with the Deactivate User box checked under 5. Action Requested. This will allow the HQ Security Officer to deactivate the user accounts. Otherwise, the system will automatically lock their passwords or deactivate their accounts as specified in the item below pertaining to "User Password Lock for Inactivity and Revocation of User Account."

V. Procedures for Requesting and Obtaining Access to SAMH and IRAS Systems

1. Any person requesting access to the SAMH system must complete, sign and submit the four (4) specific documents listed above in item IV.1.a. Copies of the forms are available online at http://www.myflfamilies.com/service-programs/substance-abuse/SAMHIS/data-forms. Online Security Awareness and HIPAA training is available at: http://www.myflfamilies.com/general-information/dcf-training.

2. Request packets should be submitted as outlined in the table below.

Private, licensed substance abuse providers, Private Seclusion/Restraint reporters, and Subcontracted providers for non-contract related IRAS/SANDR reports	
Regions/Circuits	**Submit Request Packets to:**
Central Region: Circuits 5, 9, 10, 18 NW Region: Circuits 1, 2, 14 NE Region: Circuit 3 (Madison/Taylor Co. only) Suncoast Region: Circuits 6, 12, 13, 20 Southeast Region: Circuits 15, 17, 19 Southern Region: Circuits 11, 16	Sarah.Griffith@myflfamilies.com
NE Region: Circuits 3 (excluding Madison/Taylor Co.), 4, 7, 8	James.Lynam@myflfamilies.com

Managing Entity Staff and Subcontracted Provider Staff	**Access Requested**	**Submit Request Packets to:**
Big Bend Community-Based Care	SAMHIS (TANF, SANDR, DC Aftercare), IRAS	Roderick.Harris@bigbendcbc.org
Broward Behavioral Health Coalition	SAMHIS (TANF, DC Aftercare), IRAS	Andrew.McAllister@concordiabh.org
Central Florida Behavioral Health Network	SAMHIS (TANF, DC Aftercare)	JAhrens@cfbhn.org
Central Florida Cares Health System	SAMHIS (SANDR, TANF, DC Aftercare)	MLupton@cfchs.org

Lutheran Services Florida	SAMHIS (TANF, SANDR, DC Aftercare), IRAS	James.Lynam@myflfamilies.com
South Florida Behavioral Health Network	SAMHIS (TANF, SANDR, DC Aftercare), IRAS	jguimaraes@sfbhn.com
Southeast Florida Behavioral Health Network	SAMHIS (TANF, DC Aftercare), IRAS	Andrew.McAllister@concordiabh.org

VI. Procedures for User Password Lock for Inactivity and Revocation of User Account

For users who do not routinely access SAMHIS, i.e., do not log into the system to perform any activity, their passwords will be locked out automatically by the system and their accounts will be deactivated as follows:

1. After 45 consecutive days of inactivity, the password will be locked out. Users whose passwords are locked out of the system in this manner or who forgot their passwords can have their passwords reset by contacting the Help Desk or their Regional/Managing Entity Data Liaison, or SAMH Security Officer for assistance.

Private, licensed substance abuse providers and Private Seclusion/Restraint reporters	
Regions/Circuits	**Password Reset Contacts**
Central Region: Circuits 5, 9, 10, 18 NW Region: Circuits 1, 2, 14 NE Region: Circuit 3 (Madison/Taylor Co. only) Suncoast Region: Circuits 6, 12, 13, 20 Southeast Region: Circuits 15, 17, 19 Southern Region: Circuits 11, 16	DCF HelpDesk (850-487-9400) Sarah.Griffith@myflfamilies.com
NE Region: Circuits 3 (excluding Madison/Taylor Co.), 4, 7, 8	James.Lynam@myflfamilies.com DCF HelpDesk (850-487-9400)

Managing Entity Staff and Subcontracted Provider Staff	**Password Reset Contacts**
Big Bend Community-Based Care	Roderick.Harris@bigbendcbc.org DCF HelpDesk (850-487-9400)
Broward Behavioral Health Coalition	Andrew.McAllister@concordiabh.org DCF HelpDesk (850-487-9400)
Central Florida Behavioral Health Network	JAhrens@cfbhn.org DCF HelpDesk (850-487-9400)
Central Florida Cares Health System	MLupton@cfchs.org DCF HelpDesk (850-487-9400)
Lutheran Services Florida	James.Lynam@myflfamilies.com DCF HelpDesk (850-487-9400)
South Florida Behavioral Health Network	jguimaraes@sfbhn.com DCF HelpDesk (850-487-9400)
Southeast Florida Behavioral Health Network	Andrew.McAllister@concordiabh.org DCF HelpDesk (850-487-9400)

2. After 60 consecutive days of inactivity, the user account will be revoked. The system provides User Lockout reports for password lockout and user account revocation, which will be accessible to supervisors and security SAMH Administrators at all levels (state, circuit/region and Managing Entity) for their review. Each quarter, within 15 days following the end of the quarter, the SAMH Security Officer will review the User Lockout report for users locked out due to 60 days inactivity.

a. The SAMH Security Officer will email non-contracted users notifying them of their lockout and impending revocation. To avoid revocation, documentation outlined in IV.1.a. must be submitted to the appropriate Regional Data Liaison or SAMH Security Officer (see V.2.) within 5 days.

b. The SAMH Security Officer will email designated managing entity contacts a list of all agency and subprovider users locked out with impending revocation. To avoid revocation, documentation outlined in IV.1.a. must be submitted to the appropriate Regional/Managing Entity Data Liaison or SAMH Security Officer (See V.2.) within 5 days.

c. All correspondence from the SAMHIS Security Officer regarding user accounts for which a response is not received within 5 days will result in revocation of the user account.

VII. Database Access Request Form Instructions

1. REQUESTER INFORMATION

- Insert First name, Middle Initial and Last name of individual requesting access.
- Insert Social Security Number (SSN).
- Insert Contractor ID: Managing Entity Federal ID Tax Number (9 digits). Leave blank if not Managing Entity or Managing Entity Subcontractor employee.
- Insert Provider ID: Federal Tax ID Number (FEIN), 9 digits
- Insert Provider Name:
- Insert region name, judicial circuit code (1-20), and the name of county where site is located
- Insert phone number with area code
- Fax number is optional.
- Insert email address.
- Insert Agency Mailing address: Must reflect the business location of the requestor
- DCF Issued Log-on: Leave blank unless requestor already has a 7 character alpha-numeric Department issued logon.

2. AUTHORIZATION SIGNATURES

- Supervisor's Name, Signature, and Signature Date must be completed
- SAMH/ME Data Liaison Name: Leave blank unless instructed to send request packet to Managing Entity or Regional Data Liaison.
- HQ Security Officer: Leave blank

3. DATABASE SYSTEM(S) TO BE ACCESSED BY THE REQUESTER

Check all system(s) for which access is needed. If applying only for IRAS, check only the IRAS box.

4. LEVEL AND ROLE OF THE REQUESTER:

a. **SAMHIS Roles**: For SAMHIS access, select User Level and Role for each system for which you are requesting access. For IRAS access, leave blank.

b. **IRAS Roles**: Choose one. To enter and update incidents, choose Incident Coordinator role. The Department of Children and Families Operating Procedure 215-6 requires a minimum of one (1) active user per agency. In an effort to maintain compliance for timely reporting with adequate reporting coverage, the Office of Substance Abuse and Mental Health recommends a minimum of two (2) active IRAS users.

5. ACTION REQUESTED

- Add New User is only selected when a user is being added for the first time. Do note select this option if the user requesting access already has or has had an LDAP user logon.
- Deactivate User is selected when a user is no longer with the agency or a change in job duties no longer requires access. (The agency must immediately notify the Regional/Managing Entity Data Liaison or SAMH Security Officer of the user's separation from the agency and submit a completed Database Access Request Form with the Deactivate User box checked).
- Reactivate User is selected when the user requesting access has previously had an active LDAP user logon.
- Update user information is selected when the user needs to indicate a change in any of the fields on the Database Access Request Form (i.e., name change, change in user type, employer, etc.).

5. CONFIDENTIALITY AND SECURITY REQUIREMENTS/CERTIFICATIONS:

- Type in dates of Security Awareness and HIPAA training
- Requestor's Signature and Date: Must be signed and dated by requestor.

SAMHIS User Password Lockout for Inactivity and Procedures for Revocation of User Account

For users who do not log into SAMHIS to perform any activity for 45 consecutive days, their password will be locked out. Users who are locked out due to inactivity or who forget their password may have their passwords reset by the DCF HelpDesk (850-487-9400) or their Regional/Managing Entity Data Liaison.

Users who do not log into SAMHIS for 60 consecutive days of inactivity will be revoked in SAMHIS. The user or their Managing Entity, if appropriate, will be contacted by email notifying them of the pending revocation, and users will be given 5 days to submit a new Database Access Request Form, Security Agreement Form, and current Security Awareness and HIPAA training certificates to their Regional/Managing Entity Data Liaison or SAMHIS Security Officer. All users who have not responded within 5 days will be revoked.

DCF Security Agreement Form

Each person, who requests access to SAMH data or to any departmental data, must sign the DCF Security Agreement Form (CF 114). By signing this form, the requester affirms that he/she has read the basic security safeguards as stated in this chapter. By this signature, the user also affirms that he/she has completed the computer based Security Awareness Training program, and he/she is aware of both federal and state laws pertaining to data security as listed on the form.

VIII. Database Access Request Form (see next page)

DATABASE ACCESS REQUEST FORM

This form should be typed or printed legibly and printed out for signatures. All information must be completed with the exception of Fax and DCF Log-on where not applicable.

1. REQUESTER INFORMATION:

Name: First: _____ MI: ____ Last: _____ User SSN: _____

Contractor ID (9 digit FEIN): _____ Contractor Name: _____

Provider ID (9 digit FEIN): _____ Provider Name: _____

Region: _____ Circuit: _____ County: _____ Phone: _____

Fax: _____ Email: _____

Mailing Address: _____

DCF Issued Log-on (If already assigned): _____

2. AUTHORIZATION SIGNATURES:

Supervisor's Name: _____

Supervisor's Signature: _____ **Signature Date:** _____

SAMH/ME Data Liaison Name: _____

⇒ SAMH Data Liaison or Regional Security Officer Signature: _____ Signature Date: _____

⇒ SAMH HQ Security Officer Signature: _____ Signature Date: _____

3. DATABASE SYSTEM(S) TO BE ACCESSED BY THE REQUESTER:

☐**SAMHIS Database:** ☐**Query Facility** ☐**TANF** ☐**SANDR (Seclusion-Restraint)** ☐**DC Aftercare Referral**
☐**IRAS (Incident Reporting)**

4. LEVEL AND ROLE OF THE REQUESTER:

A. SAMHIS Roles: (Choose one)

	Administrator	**Staff**
State		
Region/Circuit		
Contractor		
Sub-Contractor/Provider		
DC Facility		

B. IRAS Roles: (Choose one) ☐ **Incident Coordinator** ☐ **Viewer**

5. ACTION REQUESTED:

☐ **Add New User** ☐ **Deactivate User** ☐ **Reactivate User** ☐ **Update User Information**

6. CONFIDENTIALITY AND SECURITY REQUIREMENTS/CERTIFICATIONS:

By my signature, I acknowledge that I am responsible for safeguarding the confidentiality and security of **all** information contained in **any** of the above data systems (# 3. above) to which I am granted access as required by the following state and federal laws:

42 Code of Federal Regulation Part 2 and Part 142;
Section 394.4615, Florida Statutes;
Section 916.107(8), Florida Statutes;
45 Code of Federal Regulation Parts 160 and 164;
Section 397.501(7), Florida Statutes;
Section 282.318, Florida Statutes

I received Security Awareness Training on: _____ (MMDDYY) and HIPAA Training on: _____ (MMDDYY) ☐Certificates Attached

Requestor's Signature: _____ **Signature Date**: _____

IX. Security Agreement Form (see next page)

State of Florida
Department of Children and Families

SECURITY AGREEMENT FORM

FOR DEPARTMENT OF CHILDREN AND FAMILIES (DCF) EMPLOYEES AND SYSTEMS USERS

The Department of Children and Families has authorized me:

_____	_____
Name	Employer/Office/Region

To have access to sensitive data using computer-related media (e.g., printed reports, system inquiry, on-line updates, electronic copies or any photographic or magnetic media).

By my signature below, I acknowledge my understanding a security violation may result in criminal prosecution according to the provisions of Federal and State statutes and may also result in disciplinary action against me according to the department's Standards of Conduct in the Employee Handbook. Also by signing below, I acknowledge that I have received, read, understand and agree to be bound by the following:

- I understand the Florida Computer Crimes Act, Chapter 815, Florida Statutes, prohibits individuals from willfully, knowingly, and without authorization from deleting important data, or accessing, disrupting, denying use, destroying, injuring, or introducing a virus/malware on a computer, computer system, or computer network, or modifying or destroying computer data, computer programs, or their supporting documentation. Violations are not acceptable and may be subject to discipline up to and including separation and/or criminal charges.

- I understand Chapter 119.0712, Florida Statutes, provides that all personal identifying information contained in records relating to an individual's personal health or eligibility for health-related services held by the Department of Health is confidential.

- I understand Chapter 119.0712, Florida Statutes, provides that personal information contained in a motor vehicle record is confidential pursuant to the federal Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. ss. 2721 et seq. Such information may be released only as authorized by that act.

- I understand that 45 CFR §155.260, Privacy and Security of Personally Identifiable Information, requires the DCF workforce to comply with all policies and procedures developed and implemented by DCF to protect the privacy and security of Personally Identifiable Information.

- I understand the penalty provisions of Sections 7431, 7213 and 7213A of the Internal Revenue Code, which provide civil and criminal penalties for unauthorized inspection or disclosure of Federal Tax Information.
- I understand that Internal Revenue Code 6103(l)(7) provides confidentiality for FTI accessed for work related to the Social Security Act, the Food Stamp Act of 1977, or USC Title 38 and disclosure of this information is a confidentiality violation.
- I understand that DCF operating procedure CFOP 50-2, Security of Data and Information Technology Resources, outlines the processes for securely connecting to the department's network and securely using departmental data and other information technology resources, including how to report a security event.
- I understand it is the policy of DCF that no contract employee shall have access to Internal Revenue Service tax information or Florida Department of Law Enforcement managed Criminal Justice Information Security policy covered data (https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf), unless approved in writing, by name and position to access specified information, as authorized by regulation and/or statute.
- I understand it is the policy of DCF that I do not disclose personal passwords.
- I understand it is the policy of DCF that I do not obtain Department information for my own use or another person's personal use.
- I understand the viewing of employee or client data, even data that is not confidential or otherwise exempt from disclosure as a public record, without a business need constitutes misuse of access and is not acceptable and may be subject to discipline up to and including separation.
- I understand the Department of Children and Families will perform regular database queries to identify possible misuse of access.
- I will only access or view information or data for which I am authorized and have a legitimate business reason to see when performing my job duties. I shall maintain the integrity of all confidential and sensitive information accessed.

PRIVACY ACT STATEMENT: Disclosure of your social security number is voluntary, but must be provided in order to gain access to department systems. It is protected information pursuant to Section 282.318, Florida Statutes, the Security of Data and Information Technology Resources Act. The Department requests social security numbers to ensure secure access to data systems, prevent unauthorized access to confidential and sensitive information collected and stored by the Department, and provide a unique identifier in our systems.

Print Employee / System User Name	Signature Employee / System User	Date
Print Supervisor Name	Supervisor Signature	Date

AGREEMENT REFERENCES

FLORIDA STATUTES, CHAPTER 815: COMPUTER RELATED CRIMES

815.01 Short title.—The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."
History.—s. 1, ch. 78-92.
815.02 Legislative intent.—The Legislature finds and declares that:
(1) Computer-related crime is a growing problem in government as well as in the private sector.
(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.
(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.
(4) The proliferation of new technology has led to the integration of computer systems in most sectors of the marketplace through the creation of computer networks, greatly extending the reach of computer crime.
(5) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.
History.—s. 1, ch. 78-92; s. 2, ch. 2014-208.

815.03 Definitions.—As used in this chapter, unless the context clearly indicates otherwise:
(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
(2) "Computer" means an internally programmed, automatic device that performs data processing.
(3) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions, commonly called viruses or worms, which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp or interfere with the normal operation of the computer, computer system, or computer network.
(4) "Computer network" means a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or other electronic equipment that is connected to the computer systems or electronic devices by physical or wireless telecommunication facilities.
(5) "Computer program or computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
(6) "Computer services" include, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.
(7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.
(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.
(9) "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other

portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose.
(10) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.
(11) "Intellectual property" means data, including programs.
(12) "Property" means anything of value as defined in s. 812.012 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in machine-readable or human-readable form, and any other tangible or intangible item of value.
History.—s. 1, ch. 78-92; s. 9, ch. 2001-54; s. 4, ch. 2010-117; s. 3, ch. 2014-208.

815.04 Offenses against intellectual property; public records exemption.—
(1) A person who willfully, knowingly, and without authorization introduces a computer contaminant or modifies or renders unavailable data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device commits an offense against intellectual property.
(2) A person who willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device commits an offense against intellectual property.
(3) Data, programs, or supporting documentation that is a trade secret as defined in s. 812.081, that is held by an agency as defined in chapter 119, and that resides or exists internal or external to a computer, computer system, computer network, or electronic device is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.
(4) A person who willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation that is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, computer network, or electronic device commits an offense against intellectual property.
(5)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, the person commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
History.—s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406; s. 1, ch. 2014-177; s. 4, ch. 2014-208; s. 5, ch. 2016-5; s. 20, ch. 2016-6.

815.045 Trade secret information.—The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets.
History.—s. 2, ch. 94-100. Note.—Former s. 119.165.

815.06 Offenses against users of computers, computer systems, computer networks, and electronic devices.—
(1) As used in this section, the term "user" means a person with the authority to operate or maintain a computer, computer system, computer network, or electronic device.

(2) A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization:
(a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized;
(b) Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;
(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, computer network, or electronic device;
(d) Destroys, injures, or damages any computer, computer system, computer network, or electronic device;
(e) Introduces any computer contaminant into any computer, computer system, computer network, or electronic device; or
(f) Engages in audio or video surveillance of an individual by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device, including accessing the data or information of a computer, computer system, computer network, or electronic device that is stored by a third party.
(3)(a) Except as provided in paragraphs (b) and (c), a person who violates subsection (2) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(b) A person commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if he or she violates subsection (2) and:
1. Damages a computer, computer equipment or supplies, a computer system, or a computer network and the damage or loss is at least $5,000;
2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property;
3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service; or
4. Intentionally interrupts the transmittal of data to or from, or gains unauthorized access to, a computer, computer system, computer network, or electronic device belonging to any mode of public or private transit, as defined in s. 341.031.
(c) A person who violates subsection (2) commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the violation:
1. Endangers human life; or
2. Disrupts a computer, computer system, computer network, or electronic device that affects medical equipment used in the direct administration of medical care or treatment to a person.
(4) A person who willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, computer network, or electronic device commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.
(5)(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment or supplies, electronic device, or computer data may bring a civil action against a person convicted under this section for compensatory damages.
(b) In an action brought under this subsection, the court may award reasonable attorney fees to the prevailing party.
(6) A computer, computer system, computer network, computer software, computer data, or electronic device owned by a defendant that is used during the commission of a violation of this section or a computer or electronic device owned by the defendant that is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701-932.704.
(7) This section does not apply to a person who:
(a) Acts pursuant to a search warrant or to an exception to a search warrant authorized by law;
(b) Acts within the scope of his or her lawful employment; or
(c) Performs authorized security operations of a government or business.
(8) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, computer network, or electronic device in one

jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, computer network, or electronic device in both jurisdictions.
(9) This chapter does not impose liability on a provider of an interactive computer service as defined in 47 U.S.C. s. 230(f), information service as defined in 47 U.S.C. s. 153, or communications service as defined in s. 202.11 that provides the transmission, storage, or caching of electronic communications or messages of others; other related telecommunications or commercial mobile radio service; or content provided by another person.
History.—s. 1, ch. 78-92; s. 11, ch. 2001-54; s. 5, ch. 2014-208.

815.061 Offenses against public utilities.—
(1) As used in this section, the term “public utility” includes:
(a) A public utility or electric utility as defined in s. 366.02.
(b) A utility as defined in s. 367.021.
(c) A natural gas transmission company as defined in s. 368.103.
(d) A person, corporation, partnership, association, public agency, municipality, cooperative, gas district, or other legal entity and their lessees, trustees, or receivers, now or hereafter owning, operating, managing, or controlling gas transmission or distribution facilities or any other facility supplying or storing natural or manufactured gas or liquefied gas with air admixture or any similar gaseous substances by pipeline to or for the public within this state.
(e) A separate legal entity created under s. 163.01 and composed of any of the entities described in this subsection for the purpose of providing utility services in this state, including wholesale power and electric transmission services.
(2) A person may not willfully, knowingly, and without authorization:
(a) Gain access to a computer, computer system, computer network, or electronic device owned, operated, or used by a public utility while knowing that such access is unauthorized.
(b) Physically tamper with, insert a computer contaminant into, or otherwise transmit commands or electronic communications to a computer, computer system, computer network, or electronic device that causes a disruption in any service delivered by a public utility.
(3)(a) A person who violates paragraph (2)(a) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(b) A person who violates paragraph (2)(b) commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
History.—s. 6, ch. 2014-208.

815.07 This chapter not exclusive.—The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter. History.—s. 1, ch. 78-92.

The Driver Privacy Protection Act

18 USC 2721, Title 18-CRIMES AND CRIMINAL PROCEDURE, PART I-CRIMES
CHAPTER 123 - PROHIBITION ON RELEASE AND USE OF CERTAIN PERSONAL INFORMATION FROM STATE MOTOR VEHICLE RECORDS

Under Florida law, motor vehicle, driver license and vehicular crash record information are public information. The Driver Privacy Protection Act, 18 United States Code, Section 2721, keeps personal information private by limiting those who can have it. DPPA restricts public access to social security numbers, driver license or identification card numbers, names, addresses, telephone numbers and medical or disability information, contained in motor vehicle and driver license records. Additionally, emergency contact information and email addresses are restricted pursuant to Section 119.0712(2), Florida Statutes.

(a) In General.-A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:
(1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
(2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States.
(b) Permissible Uses.-Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321–331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows:
(1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
(2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
(3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only-
(A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
(B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
(4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
(5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
(6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
(7) For use in providing notice to the owners of towed or impounded vehicles.

(8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.
(9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.
(10) For use in connection with the operation of private toll transportation facilities.
(11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
(12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
(13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
(14) For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.
(c) Resale or Redisclosure.-An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.
(d) Waiver Procedures.-A State motor vehicle department may establish and carry out procedures under which the department or its agents, upon receiving a request for personal information that does not fall within one of the exceptions in subsection (b), may mail a copy of the request to the individual about whom the information was requested, informing such individual of the request, together with a statement to the effect that the information will not be released unless the individual waives such individual's right to privacy under this section.
(e) Prohibition on Conditions.-No State may condition or burden in any way the issuance of an individual's motor vehicle record as defined in 18 U.S.C. 2725(1) to obtain express consent. Nothing in this paragraph shall be construed to prohibit a State from charging an administrative fee for issuance of a motor vehicle record.

(Added Pub. L. 103–322, title XXX, §300002(a), Sept. 13, 1994, 108 Stat. 2099 ; amended Pub. L. 104–287, §1, Oct. 11, 1996, 110 Stat. 3388 ; Pub. L. 104–294, title VI, §604(b)(46), Oct. 11, 1996, 110 Stat. 3509 ; Pub. L. 106–69, title III, §350(c), (d), Oct. 9, 1999, 113 Stat. 1025 ; Pub. L. 106–346, §101(a) [title III, §309(c)–(e)], Oct. 23, 2000, 114 Stat. 1356 , 1356A-24.)

FLORIDA STATUTES, CHAPTER 119: PUBLIC RECORDS: DRIVER PRIVACY PROTECTION ACT (DPPA)

UNDER STATE LAW, MOTOR VEHICLE, DRIVER LICENSE, AND VEHICULAR CRASH RECORDS ARE SUBJECT TO PUBLIC DISCLOSURE; THIS STATUTE KEEPS PERSONAL INFORMATION PRIVATE BY LIMITING WHO HAS ACCESS TO THE INFORMATION.

119.0712 Executive branch agency-specific exemptions from inspection or copying of public records.—

(1) **DEPARTMENT OF HEALTH.—**All personal identifying information contained in records relating to an individual's personal health or eligibility for health-related services held by the Department of Health is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, except as otherwise provided in this subsection. Information made confidential and exempt by this subsection shall be disclosed:

(a) With the express written consent of the individual or the individual's legally authorized representative.

(b) In a medical emergency, but only to the extent necessary to protect the health or life of the individual.

(c) By court order upon a showing of good cause.

(d) To a health research entity, if the entity seeks the records or data pursuant to a research protocol approved by the department, maintains the records or data in accordance with the approved protocol, and enters into a purchase and data-use agreement with the department, the fee provisions of which are consistent with s. 119.07(4). The department may deny a request for records or data if the protocol provides for intrusive follow-back contacts, has not been approved by a human studies institutional review board, does not plan for the destruction of confidential records after the research is concluded, is administratively burdensome, or does not have scientific merit. The agreement must restrict the release of any information that would permit the identification of persons, limit the use of records or data to the approved research protocol, and prohibit any other use of the records or data. Copies of records or data issued pursuant to this paragraph remain the property of the department.

(2) **DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.—**

(a) For purposes of this subsection, the term "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by the Department of Highway Safety and Motor Vehicles.

(b) Personal information, including highly restricted personal information as defined in 18 U.S.C. s. 2725, contained in a motor vehicle record is confidential pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Such information may be released only as authorized by that act; however, information received pursuant to that act may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

(c) E-mail addresses collected by the Department of Highway Safety and Motor Vehicles pursuant to s. 319.40(3), s. 320.95(2), or s. 322.08(9) are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption applies retroactively. This paragraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2020, unless reviewed and saved from repeal through reenactment by the Legislature.

(d)1. Emergency contact information contained in a motor vehicle record is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

2. Without the express consent of the person to whom such emergency contact information applies, the emergency contact information contained in a motor vehicle record may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency.

(3) **OFFICE OF FINANCIAL REGULATION**.—The following information held by the Office of Financial Regulation before, on, or after July 1, 2011, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

(a) Any information received from another state or federal regulatory, administrative, or criminal justice agency that is otherwise confidential or exempt pursuant to the laws of that state or pursuant to federal law.

(b) Any information that is received or developed by the office as part of a joint or multiagency examination or investigation with another state or federal regulatory, administrative, or criminal justice agency. The office may obtain and use the information in accordance with the conditions imposed by the joint or multiagency agreement. This exemption does not apply to information obtained or developed by the office that would otherwise be available for public inspection if the office had conducted an independent examination or investigation under Florida law.

History.—s. 1, ch. 97-185; s. 1, ch. 2001-108; ss. 1, 2, ch. 2004-62; s. 7, ch. 2004-335; ss. 32, 33, ch. 2005-251; s. 1, ch. 2006-199; s. 1, ch. 2007-94; ss. 1, 2, ch. 2009-153; s. 1, ch. 2011-88; s. 7, ch. 2013-18; s. 1, ch. 2015-32; s. 9, ch. 2016-10; s. 1, ch. 2016-28.

Note.—

A. Additional exemptions from the application of this section appear in the General Index to the Florida Statutes under the heading “Public Records.”

B. Former s. 119.07(6)(aa), (cc).

Section 155.260: Privacy and security of personally identifiable information.
TITLE 45—Public Welfare
Subtitle A—DEPARTMENT OF HEALTH AND HUMAN SERVICES
SUBCHAPTER A—GENERAL ADMINISTRATION

(a) Creation, collection, use and disclosure.

(1) Where the Exchange creates or collects personally identifiable information for the purposes of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs, as defined in §155.300; or determining eligibility for exemptions from the individual shared responsibility provisions in section 5000A of the Code, the Exchange may only use or disclose such personally identifiable information to the extent such information is necessary:
(i) For the Exchange to carry out the functions described in §155.200;
(ii) For the Exchange to carry out other functions not described in paragraph (a)(1)(i) of this section, which the Secretary determines to be in compliance with section 1411(g)(2)(A) of the Affordable Care Act and for which an individual provides consent for his or her information to be used or disclosed; or
(iii) For the Exchange to carry out other functions not described in paragraphs (a)(1)(i) and (ii) of this section, for which an individual provides consent for his or her information to be used or disclosed, and which the Secretary determines are in compliance with section 1411(g)(2)(A) of the Affordable Care Act under the following substantive and procedural requirements:

(A) Substantive requirements. The Secretary may approve other uses and disclosures of personally identifiable information created or collected as described in paragraph (a)(1) of this section that are not described in paragraphs (a)(1)(i) or (ii) of this section, provided that HHS determines that the information will be used only for the purposes of and to the extent necessary in ensuring the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act, and that the uses and disclosures are also permissible under relevant law and policy.

(B) Procedural requirements for approval of a use or disclosure of personally identifiable information. To seek approval for a use or disclosure of personally identifiable information created or collected as described in paragraph (a)(1) of this section that is not described in paragraphs (a)(1)(i) or (ii) of this section, the Exchange must submit the following information to HHS:
(1) Identity of the Exchange and appropriate contact persons;
(2) Detailed description of the proposed use or disclosure, which must include, but not necessarily be limited to, a listing or description of the specific information to be used or disclosed and an identification of the persons or entities that may access or receive the information;
(3) Description of how the use or disclosure will ensure the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act; and
(4) Description of how the information to be used or disclosed will be protected in compliance with privacy and security standards that meet the requirements of this section or other relevant law, as applicable.

(2) The Exchange may not create, collect, use, or disclose personally identifiable information unless the creation, collection, use, or disclosure is consistent with this section.

(3) The Exchange must establish and implement privacy and security standards that are consistent with the following principles:
(i) Individual access. Individuals should be provided with a simple and timely means to access and obtain their personally identifiable information in a readable form and format;
(ii) Correction. Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable information and to have erroneous information corrected or to have a dispute documented if their requests are denied;
(iii) Openness and transparency. There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information;

(iv) Individual choice. Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable information;
(v) Collection, use, and disclosure limitations. Personally identifiable information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;
(vi) Data quality and integrity. Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner;
(vii) Safeguards. Personally identifiable information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and,
(viii) Accountability. These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

(4) For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—
(i) The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange;
(ii) Personally identifiable information is only used by or disclosed to those authorized to receive or view it;
(iii) Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section 6103 of the Code;
(iv) Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;
(v) Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and
(vi) Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules;

(5) The Exchange must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.
(6) The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically.

(b) Application to non-Exchange entities—
(1) Non-Exchange entities. A non-Exchange entity is any individual or entity that:
(i) Gains access to personally identifiable information submitted to an Exchange; or
(ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.
(2) Prior to any person or entity becoming a non-Exchange entity, Exchanges must execute with the person or entity a contract or agreement that includes:
(i) A description of the functions to be performed by the non-Exchange entity;
(ii) A provision(s) binding the non-Exchange entity to comply with the privacy and security standards and obligations adopted in accordance with paragraph (b)(3) of this section, and specifically listing or incorporating those privacy and security standards and obligations;
(iii) A provision requiring the non-Exchange entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with paragraph (a)(5) of this section;
(iv) A provision requiring the non-Exchange entity to inform the Exchange of any change in its administrative, technical, or operational environments defined as material within the contract; and
(v) A provision that requires the non-Exchange entity to bind any downstream entities to the same privacy and security standards and obligations to which the non-Exchange entity has agreed in its contract or agreement with the Exchange.

(3) When collection, use or disclosure is not otherwise required by law, the privacy and security standards to which an Exchange binds non-Exchange entities must:
(i) Be consistent with the principles and requirements listed in paragraphs (a)(1) through (6) of this section, including being at least as protective as the standards the Exchange has established and implemented for itself in compliance with paragraph (a)(3) of this section;
(ii) Comply with the requirements of paragraphs (c), (d), (f), and (g) of this section; and
(iii) Take into specific consideration:
(A) The environment in which the non-Exchange entity is operating;
(B) Whether the standards are relevant and applicable to the non-Exchange entity's duties and activities in connection with the Exchange; and
(C) Any existing legal requirements to which the non-Exchange entity is bound in relation to its administrative, technical, and operational controls and practices, including but not limited to, its existing data handling and information technology processes and protocols.

(c) Workforce compliance. The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section.

(d) Written policies and procedures. Policies and procedures regarding the creation collection, use, and disclosure of personally identifiable information must, at minimum:

(1) Be in writing, and available to the Secretary of HHS upon request; and
(2) Identify applicable law governing collection, use, and disclosure of personally identifiable information.

(e) Data sharing. Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information must:
(1) Meet any applicable requirements described in this section;
(2) Meet any applicable requirements described in section 1413(c)(1) and (c)(2) of the Affordable Care Act;
(3) Be equal to or more stringent than the requirements for Medicaid programs under section 1942 of the Act; and
(4) For those matching agreements that meet the definition of “matching program” under 5 U.S.C. 552a(a)(8), comply with 5 U.S.C. 552a(o).

(f) Compliance with the Code. Return information, as defined in section 6103(b)(2) of the Code, must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

(g) Improper use and disclosure of information. Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a CMP of not more than $25,000 as adjusted annually under 45 CFR part 102 per person or entity, per use or disclosure, consistent with the bases and process for imposing civil penalties specified at §155.285, in addition to other penalties that may be prescribed by law.

[77 FR 18444, Mar. 27, 2012, as amended at 77 FR 31515, May 29, 2012; 79 FR 13837, Mar. 11, 2014; 79 FR 30346, May 27, 2014; 81 FR 12341, Mar. 8, 2016; 81 FR 61581, Sept. 6, 2016]

Section 7213: Unauthorized disclosure of information
26 U.S.C., United States Code, 2015 Edition,
Title 26 - INTERNAL REVENUE CODE, Subtitle F - Procedure and Administration
CHAPTER 75-CRIMES, OTHER OFFENSES, AND FORFEITURES, Subchapter A-Crimes,
PART I-GENERAL PROVISIONS

(a) Returns and return information
(1) Federal employees and other persons
It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.
(2) State and other employees
It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i)(1)(C), (3)(B)(i), or (7)(A)(ii), (k)(10), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), (20), or (21) or (m)(2), (4), (5), (6), or (7) of section 6103 or under section 6104(c). Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.
(3) Other persons
It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.
(4) Solicitation
It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.
(5) Shareholders
It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.
(b) Disclosure of operations of manufacturer or producer
Any officer or employee of the United States who divulges or makes known in any manner whatever not provided by law to any person the operations, style of work, or apparatus of any manufacturer or producer visited by him in the discharge of his official duties shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution; and the offender shall be dismissed from office or discharged from employment.
(c) Disclosures by certain delegates of Secretary

All provisions of law relating to the disclosure of information, and all provisions of law relating to penalties for unauthorized disclosure of information, which are applicable in respect of any function under this title when performed by an officer or employee of the Treasury Department are likewise applicable in respect of such function when performed by any person who is a "delegate" within the meaning of section 7701(a)(12)(B).

(d) Disclosure of software

Any person who willfully divulges or makes known software (as defined in section 7612(d)(1)) to any person in violation of section 7612 shall be guilty of a felony and, upon conviction thereof, shall be fined not more than $5,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.

(e) Cross references

(1) Penalties for disclosure of information by preparers of returns

For penalty for disclosure or use of information by preparers of returns, see section 7216.

(2) Penalties for disclosure of confidential information

For penalties for disclosure of confidential information by any officer or employee of the United States or any department or agency thereof, see 18 U.S.C. 1905.

(Aug. 16, 1954, ch. 736, 68A Stat. 855 ; Pub. L. 85–866, title I, §90(c), Sept. 2, 1958, 72 Stat. 1666 ; Pub. L. 86–778, title I, §103(s), Sept. 13, 1960, 74 Stat. 940 ; Pub. L. 94–455, title XII, §1202(d), (h)(3), Oct. 4, 1976, 90 Stat. 1686 , 1688; Pub. L. 95–600, title VII, §701(bb)(1)(C), (6), Nov. 6, 1978, 92 Stat. 2922 , 2923; Pub. L. 96–249, title I, §127(a)(2)(D), May 26, 1980, 94 Stat. 366 ; Pub. L. 96–265, title IV, §408(a)(2)(D), June 9, 1980, 94 Stat. 468 , as amended Pub. L. 96–611, §11(a)(2)(B)(iv), Dec. 28, 1980, 94 Stat. 3574 ; Pub. L. 96–499, title III, §302(b), Dec. 5, 1980, 94 Stat. 2604 ; Pub. L. 96–611, §11(a)(4)(A), Dec. 28, 1980, 94 Stat. 3574 ; Pub. L. 97–248, title III, §356(b)(2), Sept. 3, 1982, 96 Stat. 645 ; Pub. L. 97–365, §8(c)(2), Oct. 25, 1982, 96 Stat. 1754 ; Pub. L. 98–369, div. A, title IV, §453(b)(4), div. B, title VI, §2653(b)(4), July 18, 1984, 98 Stat. 820 , 1156; Pub. L. 98–378, §21(f)(5), Aug. 16, 1984, 98 Stat. 1326 ; Pub. L. 100–485, title VII, §701(b)(2)(C), Oct. 13, 1988, 102 Stat. 2426 ; Pub. L. 100–647, title VIII, §8008(c)(2)(B), Nov. 10, 1988, 102 Stat. 3787 ; Pub. L. 101–239, title VI, §6202(a)(1)(C), Dec. 19, 1989, 103 Stat. 2228 ; Pub. L. 101–508, title V, §5111(b)(3), Nov. 5, 1990, 104 Stat. 1388–273 ; Pub. L. 104–168, title XII, §1206(b)(5), July 30, 1996, 110 Stat. 1473 ; Pub. L. 105–33, title XI, §11024(b)(8), Aug. 5, 1997, 111 Stat. 722 ; Pub. L. 105–35, §2(b)(1), Aug. 5, 1997, 111 Stat. 1104 ; Pub. L. 105–206, title III, §3413(b), July 22, 1998, 112 Stat. 754 ; Pub. L. 107–134, title II, §201(c)(10), Jan. 23, 2002, 115 Stat. 2444 ; Pub. L. 108–173, title I, §105(e)(4), title VIII, §811(c)(2)(C), Dec. 8, 2003, 117 Stat. 2167 , 2369; Pub. L. 109–280, title XII, §1224(b)(5), Aug. 17, 2006, 120 Stat. 1093 ; Pub. L. 111–148, title I, §1414(d), Mar. 23, 2010, 124 Stat. 237 ; Pub. L. 112–240, title II, §209(b)(3), Jan. 2, 2013, 126 Stat. 2326 ; Pub. L. 114–184, §2(b)(2)(C), June 30, 2016, 130 Stat. 537 .)

Section 7213A: Unauthorized inspection of returns or return information.
26 U.S.C., United States Code, 2015 Edition,
Title 26 - INTERNAL REVENUE CODE, Subtitle F - Procedure and Administration
CHAPTER 75-CRIMES, OTHER OFFENSES, AND FORFEITURES, Subchapter A-Crimes,
PART I-GENERAL PROVISIONS

(a) Prohibitions
(1) Federal employees and other persons
It shall be unlawful for-
(A) any officer or employee of the United States, or
(B) any person described in subsection (l)(18) or (n) of section 6103 or an officer or employee of any such person, willfully to inspect, except as authorized in this title, any return or return information.
(2) State and other employees
It shall be unlawful for any person (not described in paragraph (1)) willfully to inspect, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2) or under section 6104(c).
(b) Penalty
(1) In general
Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.
(2) Federal officers or employees
An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.
(c) Definitions
For purposes of this section, the terms "inspect", "return", and "return information" have the respective meanings given such terms by section 6103(b).

(Added Pub. L. 105–35, §2(a), Aug. 5, 1997, 111 Stat. 1104 ; amended Pub. L. 107–210, div. A, title II, §202(b)(3), Aug. 6, 2002, 116 Stat. 961 ; Pub. L. 109–280, title XII, §1224(b)(6), Aug. 17, 2006, 120 Stat. 1093 .)

Section 7431: Civil damages for unauthorized inspection or disclosure of returns and return information.
26 U.S.C., United States Code, 2015 Edition,
Title 26 - INTERNAL REVENUE CODE, Subtitle F - Procedure and Administration
CHAPTER 76 - JUDICIAL PROCEEDINGS, Subchapter B - Proceedings by Taxpayers and Third Parties

(a) In general

(1) Inspection or disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103 or in violation of section 6104(c), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure—

(1) which results from a good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of—

(1) the greater of—

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of—

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the costs of the action, plus

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(d) Period for bringing action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of unlawful inspection and disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of—

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or (3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return", and "return information" have the respective meanings given such terms by section 6103(b).

(g) Extension to information obtained under section 3406

For purposes of this section—

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103. For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

(h) Special rule for information obtained under section 6103(k)(9)

For purposes of this section, any reference to section 6103 shall be treated as including a reference to section 6311(e).

(Added Pub. L. 97–248, title III, §357(a), Sept. 3, 1982, 96 Stat. 645; amended Pub. L. 98–67, title I, §104(b), Aug. 5, 1983, 97 Stat. 379; Pub. L. 105–34, title XII, §1205(c)(2), Aug. 5, 1997, 111 Stat. 998; Pub. L. 105–35, §3(a)–(d)(4), (6), Aug. 5, 1997, 111 Stat. 1105, 1106; Pub. L. 105–206, title III, §3101(f), title VI, §6012(b)(3), July 22, 1998, 112 Stat. 729, 819; Pub. L. 109–280, title XII, §1224(b)(7), Aug. 17, 2006, 120 Stat. 1093.)

Section 6103: Confidentiality and disclosure of returns and return information
26 U.S.C., United States Code, 2015 Edition,
Title 26 - INTERNAL REVENUE CODE, Subtitle F - Procedure and Administration
CHAPTER 61-INFORMATION AND RETURNS, Subchapter B-Miscellaneous Provisions

(7) Disclosure of return information to Federal, State, and local agencies administering certain programs under the Social Security Act, the Food and Nutrition Act of 2008 of 1977,1 or title 38, United States Code, or certain housing assistance programs

(A) Return information from Social Security Administration

The Commissioner of Social Security shall, upon written request, disclose return information from returns with respect to net earnings from self-employment (as defined in section 1402), wages (as defined in section 3121(a) or 3401(a)), and payments of retirement income, which have been disclosed to the Social Security Administration as provided by paragraph (1) or (5) of this subsection, to any Federal, State, or local agency administering a program listed in subparagraph (D).

(B) Return information from Internal Revenue Service

The Secretary shall, upon written request, disclose current return information from returns with respect to unearned income from the Internal Revenue Service files to any Federal, State, or local agency administering a program listed in subparagraph (D).

(C) Restriction on disclosure

The Commissioner of Social Security and the Secretary shall disclose return information under subparagraphs (A) and (B) only for purposes of, and to the extent necessary in, determining eligibility for, or the correct amount of, benefits under a program listed in subparagraph (D).

(D) Programs to which rule applies

The programs to which this paragraph applies are:

(i) a State program funded under part A of title IV of the Social Security Act;

(ii) medical assistance provided under a State plan approved under title XIX of the Social Security Act or subsidies provided under section 1860D–14 of such Act;

(iii) supplemental security income benefits provided under title XVI of the Social Security Act, and federally administered supplementary payments of the type described in section 1616(a) of such Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(iv) any benefits provided under a State plan approved under title I, X, XIV, or XVI of the Social Security Act (as those titles apply to Puerto Rico, Guam, and the Virgin Islands);

(v) unemployment compensation provided under a State law described in section 3304 of this title;

(vi) assistance provided under the Food and Nutrition Act of 2008;

(vii) State-administered supplementary payments of the type described in section 1616(a) of the Social Security Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(viii)(I) any needs-based pension provided under chapter 15 of title 38, United States Code, or under any other law administered by the Secretary of Veterans Affairs;

(II) parents' dependency and indemnity compensation provided under section 1315 of title 38, United States Code;

(III) health-care services furnished under sections 1710(a)(2)(G), 1710(a)(3), and 1710(b) of such title; and

(IV) compensation paid under chapter 11 of title 38, United States Code, at the 100 percent rate based solely on unemployability and without regard to the fact that the disability or disabilities are not rated as 100 percent disabling under the rating schedule; and

(ix) any housing assistance program administered by the Department of Housing and Urban Development that involves initial and periodic review of an applicant's or participant's income, except that return information may be disclosed under this clause only on written request by the Secretary of Housing and Urban Development and only for use by officers and employees of the Department of Housing and Urban Development with respect to applicants for and participants in such programs.

Only return information from returns with respect to net earnings from self-employment and wages may be disclosed under this paragraph for use with respect to any program described in clause (viii)(IV).

Questions concerning this chapter should be directed to ***Regional/Managing Entity Data Liaisons or*** any of the following SAMH Central Program Office staff in Tallahassee either via phone or email:

- Sarah Griffith: (850) 717-4785, sarah.griffith@myflfamilies.com