Chapter 2 Privacy and Security

Table of Contents

Revision History

Version 10.1

- Updated document footers.
- Page 3 – Added requesters' middle initial.
- Page 5 – Added middle initial to Database Access Request Form
- Page 1 – Changed DCF Website Address for the Pamphlet 155-2
- Pages 2 & 3 – Added HIPAA Training Certificate to required Documents
- Page 5 – Added IRAS information and other changes to the Database Access Request Form
- Page 6 – Added an Email address and mailing address under "Procedure" # 3
- Page 6 – Changed Reference under "Authority" to 26 b
- Page 6 – Changed Contact Names
- Page 5 – Deleted "Comments"
- All – Changed District to Circuit or Region and changed District Data Liaison to SAMH Data Liaison
- Page 4 – Changed "DCF Security Agreement Form" to "Confidentiality and Security Requirements
- Page 4 - Added new instruction (21)
- Pages 7 – 13 – Updated Security Awareness Form to June 2010 version

Version 10.2

- Updated the document footer.

Version 10.3

- Updated document footers.
- Added Table of Contents
- Moved Revision History to beginning of chapter
- Database Access Request Instructions were updated.
- Security Agreement Form was updated.

I. 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 threefold:

- To provide a list of data elements that are identified as PHI by the Health Insurance Portability and Accountability Act (HIPAA) of 1996;
- 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 can be found on the Department web site at the following URL: http://www.dcf.state.fl.us/programs/samh/pubs_reports.shtml

Click on: Mental Health and Substance Abuse Measurement and Data - DCF PAM 155-2 (Tenth Edition, Version 3 - Effective September 2013) and then you will see all the chapters of the Pamphlet 155-2 listed.

II. Protected Health Information (PHI):

In accordance with Title 45, Code of Federal Regulations (CFR), Parts 160 and 164, which is the Final Rule pertaining to HIPAA Standards for Privacy of Individually Identifiable Health Information, the 18 PHI data elements are listed below. As the SAMHIS system contains some of these data elements, only authorized persons, who must protect this individually identifiable information from accidental or intentional misuse, can access it.

- Person names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, SAMH admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;

- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

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 that include, but are not limited to, the following:

- 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).
- 45 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.

III. Basic Security Safeguards:

There are several federal and state laws that govern the security requirements, including guidelines and standards to guard data integrity, confidentiality, availability, and reliability. Those that apply directly to the security of data in the SAMH system include, but are not limited to, the following:

- 45 Code of Federal Regulations (CFR), 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 & Families Operating Procedure (CFOP 50-2): Security of Data and Information Technology Resources.

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.

Each SAMH user must have a unique personal identifier (i.e., User Logon ID (LDAP) number (#)) that is assigned and controlled by the DCF Security Officer in Tallahassee. To obtain this confidential user code, the owner must complete, sign and submit four (4) specific documents: theDatabase Access Request Form, the DCF Security Agreement Form (CF114), the online Security Awareness Training Certificate and the online Health Insurance Portability and Accountability Act (HIPAA) Training Certificate as specified in the next section of this chapter.

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 in to the system for the first time and regularly thereafter as required by the department. Each SAMH user **must** complete the online Security Awareness Training module and the HIPAA Training module that is available on the DCF web site at: http://www.myflfamilies.com/about-us/dcf-training The certificates of completion

for these trainings **must** be submitted along with the Database Access Request Form and the DCF Security Agreement Form (CF114) documents previously identified.

The online Security Awareness Training module and the HIPAA Training module **must** be updated annually. In addition, all Provider employees who have access to departmental information shall comply with, and be provided a copy of 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 on file by the DCF Contracted/Managing Entity Agencies. Each Agency should provide a list of employee names and dates of completion of these trainings and Security Agreement forms to the SAMH Headquarters Security Officer in Tallahassee. Training updates will happen annually when the Department (DCF) does the mandated training.

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.

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 room that is lockable. The computer should be turned off and the room **must** be locked when the SAMH system user is not physically in the room.

Screensavers, when used, should be password protected.

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 locks and keys.

Never send SAMH data or other individually identifiable information to a fax machine number or to a printer unless you are absolutely sure that the recipient equipment is located in a secure location that is accessible only to authorized users.

While the primary method of connection to the Substance Abuse and Mental Health Information System (SAMHIS) is through the Secure Socket Layer (SSL), system users who access the SAMH system via the Virtual Private Network (VPN) must complete and submit a Communication Service Agreement (CSA) form as required by the Florida Department of Management Services (DMS), Division of Communications. The completion of this form allows authorized users to access the SAMH system.

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 either the data being submitted or the password in the body of the message.

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.

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.

IV. Procedures for Requesting and Obtaining Access to SAMH and IRAS Systems:

Any person requesting access to the SAMH system must complete, sign and submit four (4) specific documents, including the Database Access Request Form, the DCF Security Agreement Form (CF114), the Security Awareness Training Certificate of Completion, and the Health Insurance Portability and Accountability Act (HIPAA) Training Certificate of Completion. Copies of these documents are available through your Regional Data Liaison.

V. Database Access Request Form Instructions:

- REQUESTER INFORMATION:
  1. Insert First name, Middle Initial and Last name of individual requesting access.
  2. Insert Social Security Number (SSN). The disclosure of an individual's SSN is required by the Department as indicated on the form CF 114, which everyone must read and sign.
  3. Insert Contractor ID: Federal ID Tax Number (9 digits) if your agency holds a contract with Substance Abuse and Mental Health (SAMH) and Contract Agency name as indicated on the contract. If subcontracted with a Managing Entity, put the ME's federal tax ID number and name. If private, licensed substance abuse provider, leave blank.
  4. Insert Provider ID: Federal Tax ID Number (9 digits) if you provide substance abuse or mental health services and Provider Agency Name. Put your agency information here as the subcontractor if you are contracted with an ME, or if you are a private, licensed, non-contracted Substance Abuse provider, or freestanding psychiatric hospital.
  5. If the requester is a staff in a community provider agency or in a state hospital, the Provider ID must be the same as the one used for reporting client data in the SAMHIS data system. For DCF staff in central and circuit offices, leave both the Contractor ID and Provider ID blank.
  6. Insert region name, the numerical circuit code, and the name of county where site is located
  7. Insert phone number complete with area code
  8. Insert fax number and email address.
  9. Insert Agency Mailing address. (must reflect the business location of the requestor)
  10. If the requestor already has a 7 digit alpha-numeric Department issued logon, please provide it.

- AUTHORIZATION SIGNATURES:
  11. Individual requesting access must sign and date the form
  12. Supervisors name must be typed or printed on the form followed by Supervisor's signature and date.
  13. Individual requesting access must type the SAMH Data Liaison/Regional Security Officer name on the form and then submit to the SAMH Circuit/Regional office for signature if in Circuits 3, 4, 5, 7, 8, 9 or 18. If subcontracted with an ME, send to the ME Data Liaison. If private, licensed substance abuse provider, leave blank.
  14. HQ Security Officer signature is for Office use only

- DATABASE SYSTEM(S) TO BE ACCESSED BY THE REQUESTER:
  15. Indicate which system(s) necessary for access (check all that apply). If applying only for IRAS, check only the IRAS box. ATR access is limited to DCF employees.

- LEVEL AND ROLE OF THE REQUESTER:
  16. SAMHIS Roles: If requesting SAMH access, select User Level and Roles for each system to which you are requesting access. (you may only select one (1) user type for each system to which you are requesting access). Skip this if applying only for IRAS access.
  17. IRAS Roles: Choose one. To submit incidents, provider staff must choose Initiator or Incident Coordinator role. Each provider agency must have at least 2 Incident Coordinators. For programs with 24 hour care, be sure each shift has at least 2 Incident Coordinators.

- ACTION REQUESTED:

18. Add New User is only selected when you are adding a user for the first time. DO NOT SELECT THIS OPTION IF THE USER REQUESTING ACCESS ALREADY HAS OR HAS HAD AN LDAP ACCESS NUMBER
19. Deactivate User is selected when a user is no longer with the agency. (The agency **must** immediately notify the SAMH District Officer of the user's separation from the agency and submit a completed Database Access Request Form with the Deactivate User box checked)
20. Reactivate User is selected when a user is requesting access, has previously had an active LDAP access number which is currently inactive.
21. 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., marriage or divorce, change in user type, etc.

- CONFIDENTIALITY AND SECURITY REQUIREMENTS:

22. Type in dates of Security Awareness Training and HIPAA training
23. 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 above.
24. Once the CF 114 Form is signed and dated, it must be submitted along with a completed copy of the Database Access Request Form for SAMH and IRAS Users and the Completion Certificates for the Security Awareness Training and the HIPAA training.
25. Request packets should be submitted to Janice McIntyre at Janice_mcintyre@dcf.state.fl.us if in Circuits 3, 4, 5, 7 and 8. Request packets should be submitted to Eugene Carwise at Eugene_carwise@dcf.state.fl.us in Circuits 9 and 18. Private, licensed substance abuse providers should submit their packets to Sarah Griffith at sarah_griffith@dcf.state.fl.us if not in above referenced circuits. Subcontracted providers in all other circuits should submit packets to their ME Data Liaison.

VI. Database Access Request Form

DATABASE ACCESS REQUEST FORM

This form must be typed or completed on your computer and printed out for signatures in order to be processed
All information should 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: _____ Contractor Name: _____

Provider ID: _____ Provider Name: _____

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

Fax: _____ Email: _____

Mailing Address: _____

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

2. AUTHORIZATION SIGNATURES:

Supervisor's Name: _____

Supervisor's Signature: _____ Signature Date: _____

SAMH Data Liaison or Regional Security Officer 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

☐ **SAMH Database** (☐ **Query Facility,** ☐ **TANF,** ☐ **Data Visibility Reports)** ☐ **SALIS**

☐ **DC Aftercare Referral** ☐ **IRAS (Incident Reporting)** ☐ **Access To Recovery (ATR)**

4. LEVEL AND ROLE OF THE REQUESTER:

a. SAMHIS Roles: (Choose one)

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

b. IRAS Roles: (Choose one)

☐ **Viewer** ☐ **Initiator** ☐ **Incident Coordinator** ☐ **Death Review Coordinator** ☐ **Child Fatality Prevention Specialist**

☐ **Communications Designee** ☐ **Leadership** ☐ **User Administrator** ☐ **Administrator**

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 Statute

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

Requestor's Signature: _____ Signature Date: _____

VII. Policy Directive for Compliance with Security Awareness Training Requirement

A. Purpose

The purpose of this policy directive is to define how agencies, who are contracted with District Substance Abuse and Mental Health Program Offices, will comply with the completion of the Security Awareness Training requirements.

B. Authority

Each state-contracted substance abuse and mental health provider agency is required to

"*provide the latest Departmental Security Awareness Training to its staff and subcontractors who have access to departmental information*" as specified in section 26.b (Information Security Obligations) of the Florida Department of Children and Families Standard Contract.

C. Procedure

1. Security Awareness Training needs to be conducted by all state-contracted substance abuse and mental health providers. New users will have to complete the training prior to a logon user code being issued.
2. Existing users must complete and sign the new Confidentiality and Security Agreement form to indicate when the Security Awareness Training was provided. The original copy of this form should be filed in the user's personnel file and a copy of the signed form must be forwarded to the District Data Liaison. New users must complete and sign the new Confidentiality and Security Agreement form indicating they have completed the Security Awareness training before a logon user code is assigned. A copy of the new Confidentiality and Security Agreement form can be obtained from *SAMH Data Liaisons or Regional Security Officers* upon request by state-contracted provider agencies.
3. Upon receipt of the *signed agreement forms* from provider agencies, *SAMH Data Liaisons or Regional Security Officers* must forward copies of the signed agreement forms to the SAMH Central Program Office in Tallahassee by Emailing to: SAMH_IRAS_User_Accounts@dcf.state.fl.us or mailing the forms to: SAMH Performance Support – Data Section, 1317 Winewood Blvd., Bldg. 6, Tallahassee, FL. 32399
4. Any revoked access will be reinstated any time by the SAMH Central Program Office staff if the Security Awareness Training is completed and the new Confidentiality and Security Agreement form is forwarded to the *SAMH Data Liaisons or Regional Security Officers* as specified above. Central Office will continue to monitor users' compliance with keeping Security Awareness Training up to date.
5. The *Computer Based Security Awareness Training* is the departmental training method, which state-contracted agencies can use to meet the minimum training requirements.
6. The online Security Awareness Training module and the HIPAA Training module **must** be updated annually. In addition, all Provider employees who have access to departmental information shall comply with, and be provided a copy of 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 on file by the DCF Contracted/Managing Entity Agencies. Each Agency should provide a list of employee names and dates of completion of these trainings and Security Agreement forms to the DCF Headquarters Security Officer in Tallahassee. Training updates will happen annually when the Department (DCF) does the mandated training.

Questions concerning this policy should be directed to *SAMH Data Liaisons or Regional Security Officers* or any of the following SAMH Central Program Office staff in Tallahassee either via email or by phone:

Sarah Griffith
(850) 717-4785
sarah_griffith@dcf.state.fl.us

Sherry Catledge
(805) 717-4404
sherry_catledge@dcf.state.fl.us

VIII. Security Agreement Form

SECURITY AGREEMENT FORM

The Department of Children and Families has authorized you:

_____

Employee's or Other System User's Name/Organization

to have access to sensitive data using computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media).

Computer crimes are a violation of the department's Standards of Conduct. In addition to departmental discipline, committing computer crimes may result in Federal or State felony criminal charges.

I understand that 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.

By my signature below, I acknowledge that I have received, read, understand and agree to be bound by the following:

- The Computer Related Crimes Act, Chapter 815, F.S.
- Sections 7213, 7213A, and 7431 of the Internal Revenue Code, which provide civil and criminal penalties for unauthorized inspection or disclosure of Federal tax data.
- 6103(l)(7) of the Internal Revenue Code, which provides confidentiality and disclosure of returns and return information.
- CFOP 50-2.
- It is the policy of the Department of Children and Families that no contract employee shall have access to IRS tax information or FDLE information, unless approved in writing, by name and position to access specified information, as authorized by regulation and/or statute.
- It is the policy of the Department of Children and Families that I do not disclose personal passwords.
- It is the policy of the Department of Children and Families that I do not obtain information for my own or another person's personal use.
- 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 duties. I shall maintain the integrity of all confidential and sensitive information accessed.
- "Casual viewing" of employee or client data, even data that is not confidential or otherwise exempt from disclosure as a public record, constitutes misuse of access and is not acceptable.
- The Department of Children and Families will perform regular database queries to identify misuse of access.
- Chapter 119.0712, Florida Statutes, and the Driver Privacy Protection Act (DPPA).

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 requested, however, 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 or Other System User Name	Signature of Employee or Other System User	Date
Print Supervisor Name	Signature of Supervisor	Date

CF 114, PDF 03/2013 Distribution of Copies: Original – Personnel File/Other System User File; Copy – Employee/Other System User

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) 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.)

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 contaminant other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(4) "Computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by 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) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Intellectual property" means data, including programs.

(11) "Property" means anything of value as defined in [Footnote 1] s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either 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.) ([Footnote 1] Note: Repealed by s. 16, ch. 77-342.)

815.04 Offenses against intellectual property; public records exemption.

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) (a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. (b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which 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, or computer network commits an offense against intellectual property.

(4) (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, then the offender is guilty of 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.)

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 computer users.

(1) Whoever willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, or computer network; (b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or 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, or computer network; (d) Destroys, injures, or damages any computer, computer system, or computer network; or (e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.

(2) (a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (b) Whoever violates subsection (1) and: 1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is $5,000 or greater; 2. Commits the offense for the purpose of

devising or executing any scheme or artifice to defraud or obtain property; or 3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) Whoever willingly, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(4) (a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages. (b) In any action brought under this subsection, the court may award reasonable attorney fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which 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.

(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.

(7) 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, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

(History: s. 1, ch. 78-92; s. 11, ch. 2001-54.)

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.)

SECTION 7213 – UNAUTHORIZED DISCLOSURE OF INFORMATION

(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)(3)(B)(i),(1)(6),(7),(8),(9),(10),(12),(15) or (16) or (m)(2),(4),(5),(6), or (7) of section 6103. 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 cost 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 an 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 cost 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 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 cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 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 exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

SECTION 7213A – UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(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 section 6103(n) or an officer 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(l)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY –

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, 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 respective meanings given such terms by section 6103(b).

SECTION 7431 – CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION

(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 THE 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, 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 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 cost of the action.

(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.

SECTION 6103 – CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION

(l) DISCLOSURE OF RETURNS AND RETURN INFORMATION FOR PURPOSES OTHER THAN TAX ADMINISTRATION

(7) Disclosure of return information to Federal, State, and local agencies administering certain programs under the Social Security Act, the Food Stamp Act of 1977, 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 Stamp Act of 1977;

(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 section 1710(a)(1)(I), 1710(a)(2), 1710(b), and 1712(a)(2)(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). Clause (viii) shall not apply after September 30, 2008.

DRIVER PRIVACY PROTECTION ACT (DPPA)

Under state law, motor vehicle, driver license, and vehicular crash records are subject to public disclosure. The Driver Privacy Protection Act (DPPA) keeps your personal information private by limiting who has access to the information. (http://www.flhsmv.gov/ddl/DPPAInfo.html)

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

(2) DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.

(a) Personal information contained in a motor vehicle record that identifies an individual is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution except as provided in this subsection. Personal information includes, but is not limited to, an individual's social security number, driver identification number or identification card number, name, address, telephone number, medical or disability information, and emergency contact information. For purposes of this subsection, personal information does not include information relating to vehicular crashes, driving violations, and driver's status. 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 contained in motor vehicle records made confidential and exempt by this subsection may be released by the department for any of the following uses:

1. 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 nonowner 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. ss. 1231 et seq.), the Clean Air Act (42 U.S.C. ss. 7401 et seq.), and chapters 301, 305, and 321-331 of Title 49, United States Code.

2. 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.

3. 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 nonowner records from the original owner records of motor vehicle manufacturers.

4. 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.

5. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any court or agency or before any self-regulatory body for:

a. Service of process by any certified process server, special process server, or other person authorized to serve process in this state.

b. Investigation in anticipation of litigation by an attorney licensed to practice law in this state or the agent of the attorney; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

c. Investigation by any person in connection with any filed proceeding; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

d. Execution or enforcement of judgments and orders.

e. Compliance with an order of any court.

6. 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.

7. 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, anti-fraud activities, rating, or underwriting.

8. For use in providing notice to the owners of towed or impounded vehicles.

9. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection. Personal information obtained based on an exempt driver's record may not be provided to a client who cannot demonstrate a need based on a police report, court order, or business or personal relationship with the subject of the investigation.

10. 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 49 U.S.C. ss. 31301 et seq.

11. For use in connection with the operation of private toll transportation facilities.

12. For bulk distribution for surveys, marketing, or solicitations when the department has obtained the express consent of the person to whom such personal information pertains.

13. For any use if the requesting person demonstrates that he or she has obtained the written consent of the person who is the subject of the motor vehicle record.

14. For any other use specifically authorized by state law, if such use is related to the operation of a motor vehicle or public safety.

15. For any other use if the person to whom the information pertains has given express consent in a format prescribed by the department. Such consent shall remain in effect until it is revoked by the person on a form prescribed by the department.

(c) Notwithstanding paragraph (b), without the express consent of the person to whom such information applies, the following information contained in motor vehicle records may only be released as specified in this paragraph:

1. Social security numbers may be released only as provided in subparagraphs (b)2., 5., 7., and 10.

2. An individual's photograph or image may be released only as provided in s. 322.142.

3. Medical disability information may be released only as provided in ss. 322.125 and 322.126.

4. Emergency contact information may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency.

(d) The restrictions on disclosure of personal information provided by this subsection shall not in any way affect the use of organ donation information on individual driver licenses or affect the administration of organ donation initiatives in this state.

(e) 1. Personal information made confidential and exempt may be disclosed by the Department of Highway Safety and Motor Vehicles to an individual, firm, corporation, or similar business entity whose primary business interest is to resell or redisclose the personal information

to persons who are authorized to receive such information. Prior to the department's disclosure of personal information, such individual, firm, corporation, or similar business entity must first enter into a contract with the department regarding the care, custody, and control of the personal information to ensure compliance with the federal Driver's Privacy Protection Act of 1994 and applicable state laws.

2. An authorized recipient of personal information contained in a motor vehicle record, except a recipient under subparagraph (b)12., may contract with the Department of Highway Safety and Motor Vehicles to resell or redisclose the information for any use permitted under this section. However, only authorized recipients of personal information under subparagraph (b)12. may resell or redisclose personal information pursuant to subparagraph (b)12.

3. Any authorized recipient who resells or rediscloses personal information shall maintain, for a period of 5 years, records identifying each person or entity that receives the personal information and the permitted purpose for which it will be used. Such records shall be made available for inspection upon request by the department.

(f) The department may adopt rules to carry out the purposes of this subsection and the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Rules adopted by the department may provide for the payment of applicable fees and, prior to the disclosure of personal information pursuant to this subsection, may require the meeting of conditions by the requesting person for the purposes of obtaining reasonable assurance concerning the identity of such requesting person, and, to the extent required, assurance that the use will be only as authorized or that the consent of the person who is the subject of the personal information has been obtained. Such conditions may include, but need not be limited to, the making and filing of a written application in such form and containing such information and certification requirements as the department requires.

(g) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed October 2, 2012, unless reviewed and saved from repeal through reenactment by the Legislature