MEMORANDUM

Agenda Item No. 18(A)(1)

TO:	Honorable Chairman Joe A. Martinez and Members, Board of County Commissioners	**DATE:**	October 2, 2012
FROM:	R. A. Cuevas, Jr. County Attorney	**SUBJECT:**	Resolution ratifying the County Mayor's action to approve and execute a standard Memorandum of Agreement between the State of Florida Department of Children and Families Miami-Dade County and Miami-Dade County for Limited County Access to Florida System Data

The accompanying resolution was prepared by the Community Action and Human Resources Department and placed on the agenda at the request of Prime Sponsor Commissioner Rebeca Sosa.

R. A. Cuevas, Jr.
County Attorney

RAC/lmp

/

Memorandum

Date: October 2, 2012

To: Honorable Chairman Joe A. Martinez
and Members, Board of County Commissioners

From: Carlos A. Gimenez
County Mayor

Subject: Ratification of the Memorandum of Agreement between the State of Florida Department of Children and Families and Miami-Dade County for Limited County Access to Florida System Data

---

RECOMMENDATION

It is recommended that the Board of County Commissioners (Board) ratify the standard Memorandum of Agreement between Miami-Dade County and the State of Florida Department of Children and Families (DCF) for Limited County Access to Florida System Data, with the related attachments Exhibits A through D. Access to this system will assist Miami-Dade County Community Action and Human Services (the Department) staff in the review, approval and reimbursement of the shared Medicaid costs reimbursable by the County to the State of Florida after ascertaining that said costs were incurred on behalf of a Miami-Dade County resident.

SCOPE

The impact of this Memorandum of Agreement is countywide.

FISCAL IMPACT/FUNDING SOURCE

The fiscal impact to the County is minimal as the annual costs for access to the Department and Children and Families Florida System is $960.00. This amount will be covered by General Fund.

TRACK RECORD/MONITOR

The Department has been processing the shared cost Medicaid reimbursement for approximately the last thirty (30) years. The person responsible for assuring that all aspects of the MOA are complied with is Mr. Richard Signori, Special Projects Administrator 2, Community Action and Human Services Department.

BACKGROUND

The County is required to reimburse the State of Florida, on a monthly basis, for certain Medicaid costs paid by the State of Florida on behalf of Miami-Dade County residents. This requires County staff to review and verify each claim to ensure that the Medicaid recipient is a Miami-Dade County resident before reimbursement can be approved. In many instances, the addresses included in the Medicaid invoices from the state are incorrect, incomplete, have a post office box address or an address is not provided at all. Many of these errors occur because the Medicaid provider is not able to record the correct address at the time medical and nursing home services are provided to the recipient. Accordingly, staff rejects these claims as they are unable to confirm the Medicaid recipient's address, only to have to review claims again several months later when the state does correctly identify the address as a Miami-Dade County address.

During the 2012 Regular Session, the Florida Legislature enacted Chapter 2012-33, Laws of Florida (HB 5301), which changed the county Medicaid billing system to provide that the state would collect the county share of Medicaid billings through an automatic withholding of county revenue sharing and sales tax distributions. Chapter 2012-33 also required automatic withholding of county revenue sharing for backlog billings going back to 2001.

While estimates have varied, Chapter 2012-33 could cost Miami-Dade County as much as $31 million over the next few fiscal years. Per Resolution 350-12, Miami-Dade County joined other Counties and the Florida Association of Counties in filing a lawsuit challenging the Medicaid county revenue sharing mandate enacted in Chapter 2012-33, Laws of Florida, HB 5301.

Since the State of Florida Department and Children and Families maintains the Florida System database, which contains the official demographic data of each Medicaid recipient, it is necessary for staff to be able to access the Florida System and resolve these errors during the initial review of Medicaid invoices. Under the attached Memorandum of Agreement, DCF will provide the County with limited access to the Florida System and to information that is confidential to the extent required by law to verify Medicaid recipient addresses. The Memorandum of Agreement contains an indemnification provision in favor of DCF, to the extent permitted by law, including Section 768.28, Florida Statutes, and without waiving the limits of sovereign immunity.

The Department sought approval to gain access to the Department of Children and Families' Florida System which contains official demographic data regarding eligible and registered Medicaid recipients. Although the Department uses other outside databases such as the United States Postal Service's address database to confirm the vast majority of addresses attributable to Miami-Dade County Medicaid recipients, only the Florida System can provide an address based upon a Medicaid recipient's social security number.

Attachments

Russell Benford, Deputy Mayor

MEMORANDUM

(Revised)

TO: Honorable Chairman Joe A. Martinez and Members, Board of County Commissioners

DATE: October 2, 2012

FROM: R. A. Cuevas, Jr. County Attorney

SUBJECT: Agenda Item No. 18(A)(1)

Please note any items checked.

_____ "3-Day Rule" for committees applicable if raised

_____ 6 weeks required between first reading and public hearing

_____ 4 weeks notification to municipal officials required prior to public hearing

_____ Decreases revenues or increases expenditures without balancing budget

_____ Budget required

_____ Statement of fiscal impact required

_____ Ordinance creating a new board requires detailed County Manager's report for public hearing

_____ No committee review

_____ Applicable legislation requires more than a majority vote (i.e., 2/3's ____, 3/5's ____, unanimous _____) to approve

✓ Current information regarding funding source, index code and available balance, and available capacity (if debt is contemplated) required

Approved _____ Mayor
Veto _____
Override _____

Agenda Item No. 18(A)(1)
10-2-12

RESOLUTION NO. _____

RESOLUTION RATIFYING THE COUNTY MAYOR OR THE COUNTY MAYOR'S DESIGNEE ACTION TO APPROVE AND EXECUTE A STANDARD MEMORANDUM OF AGREEMENT BETWEEN THE STATE OF FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES AND MIAMI-DADE COUNTY FOR LIMITED COUNTY ACCESS TO FLORIDA SYSTEM DATA FOR THE PURPOSE OF REVIEWING, APPROVING AND REIMBURSING SHARED MEDICAID COSTS TO THE STATE OF FLORIDA; AND FURTHER AUTHORIZING THE COUNTY MAYOR OR COUNTY MAYOR'S DESIGNEE TO APPROVE AND EXECUTE ANY OTHER AGREEMENTS THAT MAY ARISE FOR THIS PURPOSE

WHEREAS, this Board desires to accomplish the purposes outlined in the accompanying memorandum, a copy of which is incorporated herein by reference; and

WHEREAS, this Board has adopted Resolution No. R-549-12, authorizing the County Mayor or County Mayor's designee to administer County business during the Board of County Commissioners' 2012 summer recess as provided therein, and has directed that all actions taken pursuant to such authority be submitted to this Board for ratification at its October 2, 2012 meeting,

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF MIAMI-DADE COUNTY, FLORIDA, that this Board ratifies the County Mayor or the County Mayor's designee action to approve and execute the Standard Memorandum of Agreement for Limited County Access to Florida System Data, attached and including Exhibits A through D, that will assist Miami-Dade County Community Action and Human Services staff in the review, approval and reimbursement of the shared Medicaid costs reimbursable by the County to the State of Florida after ascertaining that said costs were incurred on behalf of a Miami-Dade County resident; authorizes the County Mayor or County Mayor's designee to execute such contracts and agreements as are required by the State of Florida

following their review by the County Attorney's Office; to execute such other contracts as will serve to further the purposes described in the Memorandum of Agreement, and authorizes the County Mayor or County Mayor's designee to file and execute any necessary amendments to the Memorandum of Agreement for and on behalf of Miami-Dade County, Florida; and to exercise amendment, modification, renewal, cancellation and termination clauses of any contracts and agreements on behalf of Miami-Dade County, Florida.

The foregoing resolution was offered by Commissioner , who moved its adoption. The motion was seconded by Commissioner and upon being put to a vote, the vote was as follows:

Joe A. Martinez, Chairman
Audrey M. Edmonson, Vice Chairwoman

Bruno A. Barreiro	Lynda Bell
Esteban L. Bovo, Jr.	Jose "Pepe" Diaz
Sally A. Heyman	Barbara J. Jordan
Jean Monestime	Dennis C. Moss
Rebeca Sosa	Sen. Javier D. Souto
Xavier L. Suarez	

The Chairperson thereupon declared the resolution duly passed and adopted this 2nd day of October, 2012. This resolution shall become effective ten (10) days after the date of its adoption unless vetoed by the Mayor and if vetoed shall become effective only upon an override by this Board.

MIAMI-DADE COUNTY, FLORIDA
BY ITS BOARD OF
COUNTY COMMISSIONERS

HARVEY RUVIN, CLERK

By:_____
Deputy Clerk

Approved by County Attorney as
to form and legal sufficiency.

Estephanie S. Resnik

MEMORANDUM OF AGREEMENT FOR LIMITED COUNTY ACCESS TO FLORIDA SYSTEM DATA

This Memorandum of Agreement for Limited County Access to FLORIDA System data (hereinafter "MOA") is entered into between the Florida Department of Children and Families (the Department) and Miami-Dade County (the County).

WHEREAS, the Department maintains certain information in its Florida Online Recipient Integrated Data Access (FLORIDA) System regarding applicants seeking to qualify for Medicaid Services;

WHEREAS, the County needs to access limited data on the FLORIDA System to confirm limited information regarding recipients of Medicaid Services within the County for payment purposes; and

WHEREAS, the Department is willing to provide the County with limited access to the data in the FLORIDA System for such purposes, provided that the County complies with certain security requirements.

NOW THEREFORE, IT IS AGREED AS FOLLOWS:

1. The foregoing recitations are true and incorporated into the terms of this MOA by reference.

2. Conditioned on the County's compliance with the terms of "Exhibit A" to this MOA and the terms below, the Department will grant authorized County employees limited access to the FLORIDA System to verify Medicaid recipient addresses. Authorized County employees will be provided "view only" access to the screens shown in "Exhibit B" to this MOA (hereinafter the "limited FLORIDA data"). The Department will have sole discretion to determine the means of access and the manner of display of the limited FLORIDA data.

3. The County hereby agrees to comply with the terms of "Exhibit A" and will access the limited FLORIDA data exclusively for purposes of verifying Medicaid recipient addresses and will not utilize nor permit any person to utilize the limited FLORIDA data for any other purpose. Any County record of the limited FLORIDA data shall be maintained and used only in accordance with the terms of this MOA; however, the foregoing does not limit the right of the parties to enter into subsequent agreements or seek court or administrative orders authorizing the use of these records in judicial or administrative proceedings.

4. The Department will provide appropriate and timely training and support to the County, including its employees, with regard to FLORIDA System access.

5. Prior to granting access to the FLORIDA System to individual users at the County level, the following must be accomplished:
   a. The Department must be in receipt of a signed MOA with the appropriate County entity (ies).

b. The Department must be in receipt of a FLORIDA Individual Security Information Form ("Exhibit C") for each user requesting access to the FLORIDA System.

c. The Department must be in receipt of a signed DCF CF 114 "Security Agreement Form" (Exhibit D). This form should accompany Exhibit C.

d. Individual users must have received confirmation from the FLORIDA Application Data Security Administrator that access has been granted and received a user ID and an initial password.

e. Individual users have completed FLORIDA System access training.

f. Individual users shall have completed the required initial Department online security training, and have printed out their completion certificate for their local personnel file. A copy of the security-training certificate should accompany Exhibit C. This training is required annually after completion of the initial training.

6. This MOA shall commence the last day executed by all parties and shall continue for a period of five years, provided, however, that the confidentiality requirements regarding the limited FLORIDA data shall survive the expiration or termination of this MOA. This MOA may be terminated by either party without cause upon 30 days written notice. This MOA may be terminated by either party for cause upon no less than 24 hours written notice. The Department may administratively suspend access to the FLORIDA System at any time the Department has reason to believe that the County is not in full compliance with the provisions of this MOA.

7. To the extent permitted by law, including Section 768.28, Florida Statutes, and without waiving the limits of sovereign immunity, the County shall indemnify the Department, its officers, employees and agents from any suits, actions, damages, claims and costs of every name and description, including attorneys' fees, relating to access to or use of the limited FLORIDA data by the County, its officers, employees or agents; provided, however, that this indemnity shall not include that portion of any loss or damages proximately caused by an act or omission of the Department, its officers, employees or agents.

8. This MOA executed and entered into in the State of Florida, shall be construed, performed and enforced in all respects in accordance with Florida law and venue shall be in Leon County, Florida.

9. There are no provisions, terms, conditions, or obligations other than those contained herein, and this MOA shall supersede all previous communications, representations, or agreements, either verbal or written between the parties.

10. If any term or provision of this MOA is legally determined unlawful or unenforceable, the remainder of the MOA shall remain in full force and effect and such term or provision shall be stricken.

11. Modifications of provisions of this MOA shall be valid only when they have been reduced to writing and duly executed by the duly authorized officials of both parties.

12. To the extent that the Miami-Dade County Clerk of the Circuit Court acts as the County's agent or administrator for purpose of Medicaid payments to recipients, the term "County" as used in this MOA shall include the Clerk of the Circuit Court, provided that this MOA is also executed by the Clerk of the Circuit Court as provided below.

13. The parties contact coordinators for the administration of this MOA are:

County contact/coordinator:
Barbara Galvez
Operating Budget Coordinator
Miami-Dade County
111 N.W. 1st St-22nd Fl., Miami, Fl. 33128
305-375-2814
bgal@miamidade.gov

Clerk of Circuit Court contact/coordinator:
Fara Diaz
Director's Office
Miami-Dade County, Clerk of the Courts
73 West Flagler St.-Suite #242
Miami, Fl. 33130
(305) 275-1155
farad@miamidade.gov

Department contact/coordinator:
Bruce R. Belrose
Chief, Operations and Research
Florida Department of Children and Families
Economic Self-Sufficiency Program Office
1317 Winewood Boulevard, 3-426
Tallahassee, FL 32399-0700
850-717-4083
Bruce_belrose@dcf.state.fl.us

IN WITNESS THEREOF, the parties hereto have caused this Memorandum of Agreement to be executed by their undersigned officials as duly authorized.

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES

Signature Date

Ann M. Berner
Director, Economic Self-Sufficiency Program

MIAMI-DADE COUNTY MAYOR
OR MAYOR'S DESIGNEE

Signature Date

ATTEST:

MIAMI-DADE COUNTY
a political subdivision
of the State of Florida

HARVEY RUVIN, CLERK

BY: _____
DEPUTY CLERK

Carlos A. Gimenez
County Mayor

(DATE)

Attachments:

Exhibit A – Use and Security Requirements
Exhibit B – FLORIDA System screen shots
Exhibit C – FLORIDA Individual Security Information form
Exhibit D – DCF CF114 Security Agreement Form

EXHIBIT A – COUNTY USE AND SECURITY REQUIREMENTS

The County agrees to comply with the following use and security requirements:

1. Information obtained from the Department's system pursuant to the MOA (hereinafter "the limited FLORIDA data") is confidential in nature and protected from disclosure by State and Federal Law.

2. To restrict the transmission of the limited FLORIDA data using secure file transfer protocols to County personnel who have a verifiable need to know in the performance of their official duties for the purposes stated in Section 3 of the MOA.

3. To maintain a listing of County personnel granted on-line access privileges to the Department's system pursuant to this MOA and, upon request, make such information available to the Department. At a minimum, the list will include the user's first and last name, User Identification (USERID), date access was granted/changed/deleted, dates of initial security training and annual awareness training. This information will be maintained for a period of 5 years after access has been terminated or until administrative purposes have been served, whichever is longer.

4. To abide by IT Security Awareness training provided by the Department at http://www.dcf.state.fl.us/admin/training.shtml or equivalent security training provided to court IT security officers. Initial and annual refresher IT Security Awareness training shall be documented.

5. To comply with State of Florida network security requirements specified in Florida Administrative Code 60DD-2.006, Network Security.

6. The limited FLORIDA data may not be re-disclosed by the County or its personnel verbally, electronically or in any other forms except as specifically authorized by law or regulation and in compliance with 42 C.F.R., Subpart F.

7. Any limited FLORIDA data will be used only for the purposes stated in Section 3 of the MOA and may be disclosed only for such purposes.

8. The limited FLORIDA data shall be stored in a place physically secure from access by unauthorized persons.

9. To safeguard access to the limited FLORIDA data in such a way that unauthorized persons cannot view, print, copy or retrieve the information by any means.

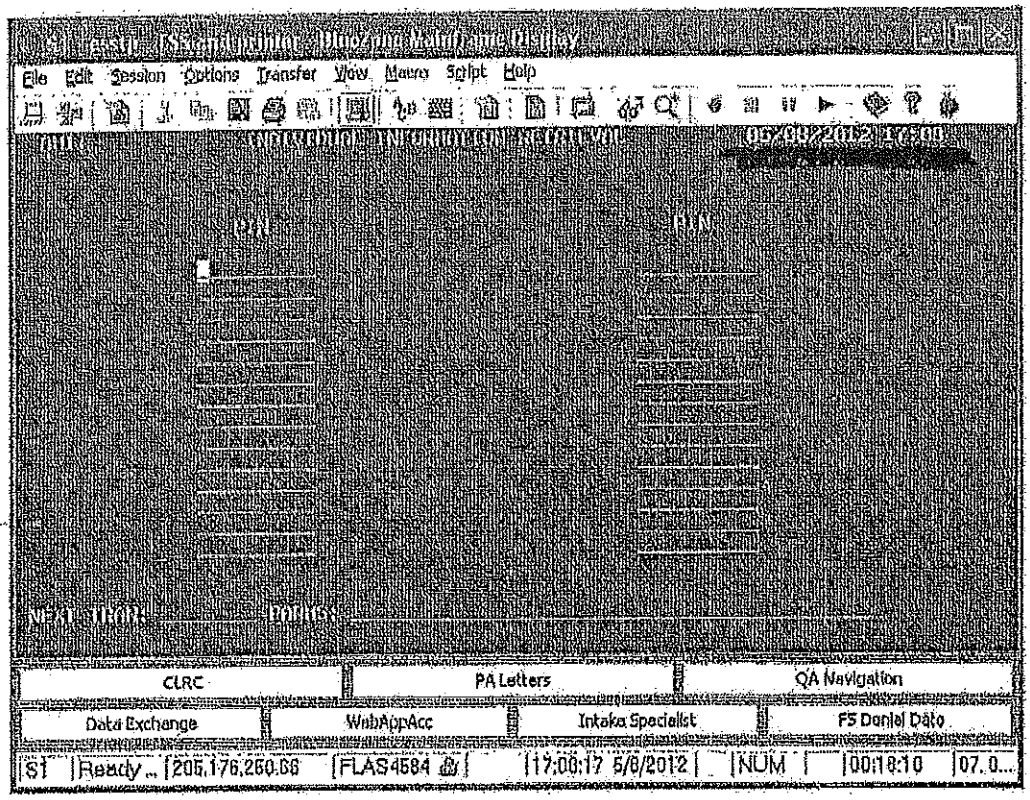
10. To instruct all personnel granted on-line access privileges to the Department's system or granted access to the limited FLORIDA data in the County's possession regarding the confidential nature of the information, the safeguards and requirements of this MOA and the provisions of Chapters 71A-1 and 71A-2, Florida Administrative Code as well as Chapters 119, 812, 815, 817, 839 or 877, Florida Statutes, or similar state and federal requirements.

11. To adhere to the confidentiality requirements stated herein, and to fully and promptly report any infraction of these requirements to the respective contacts specified in Section 10 of the MOA.

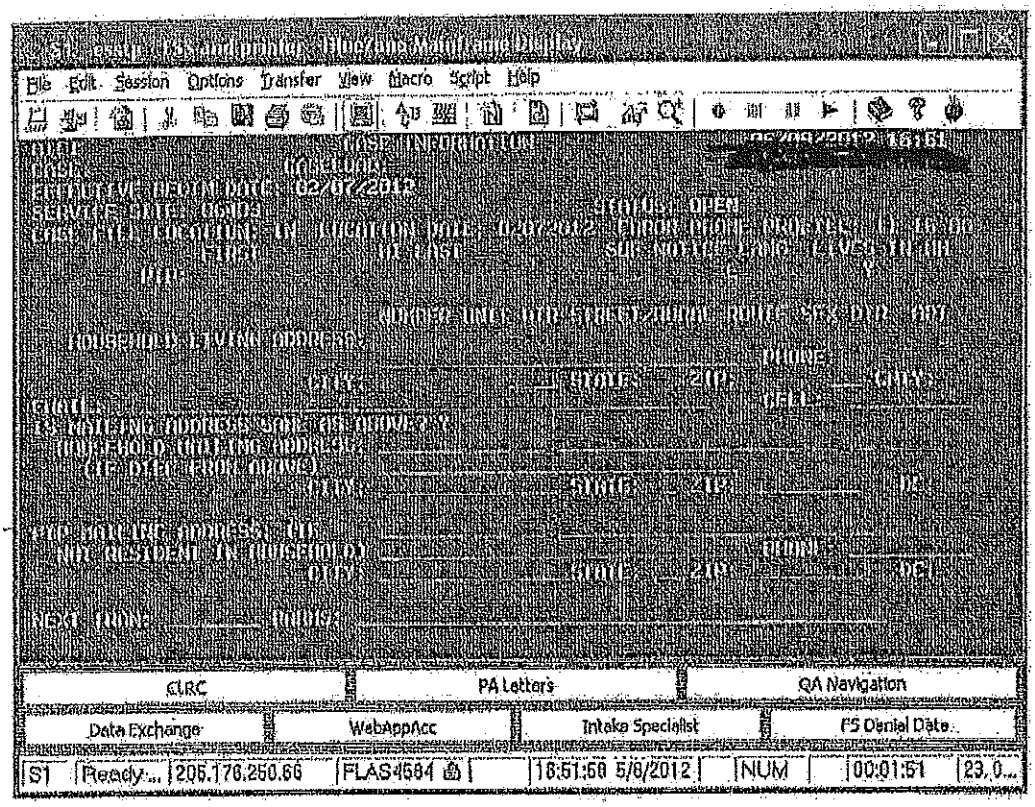
12. To promptly notify the Department of any breach of security related to the limited FLORIDA data in its possession and to be responsible for full compliance with section 817.5681, F.S., if applicable, in the event of a breach of security concerning confidential personal information in its possession received from one another, including but not limited to, providing notification to affected persons.

13. To provide any such breach notification, if applicable, to the Department for prior review and approval of the contents of the notice.

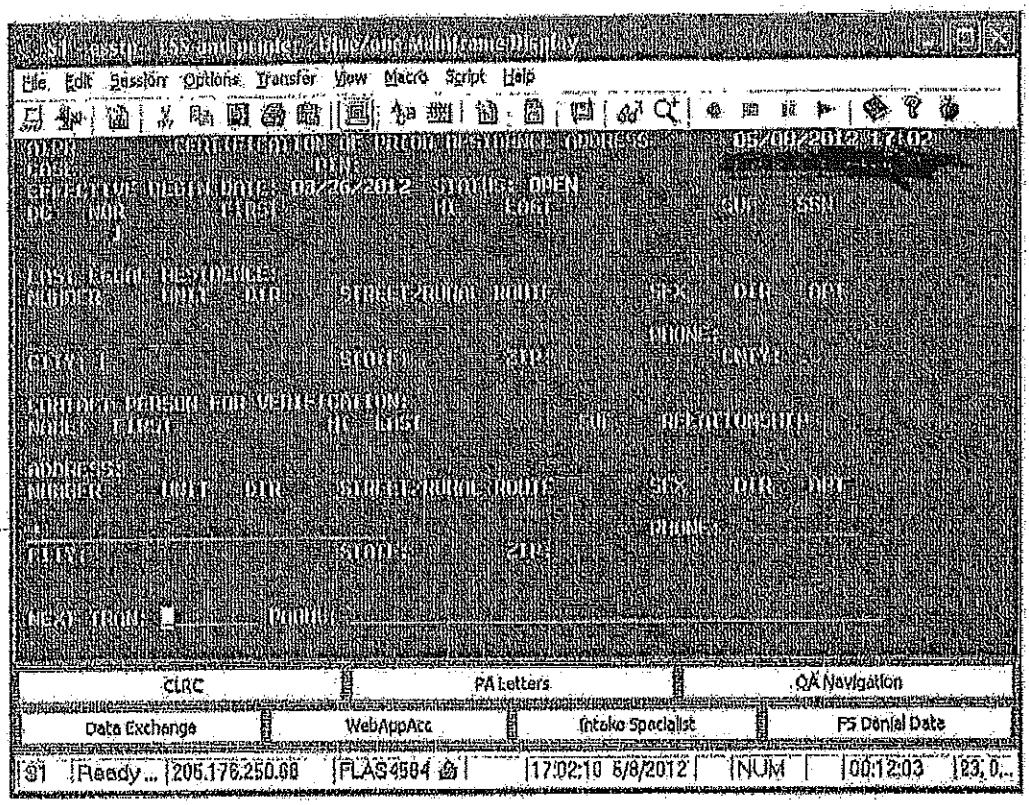
"EXHIBIT B"
Limited FLORIDA Data



"EXHIBIT B"
Limited FLORIDA Data



"EXHIBIT B"
Limited FLORIDA Data



"EXHIBIT B"
Limited FLORIDA Data

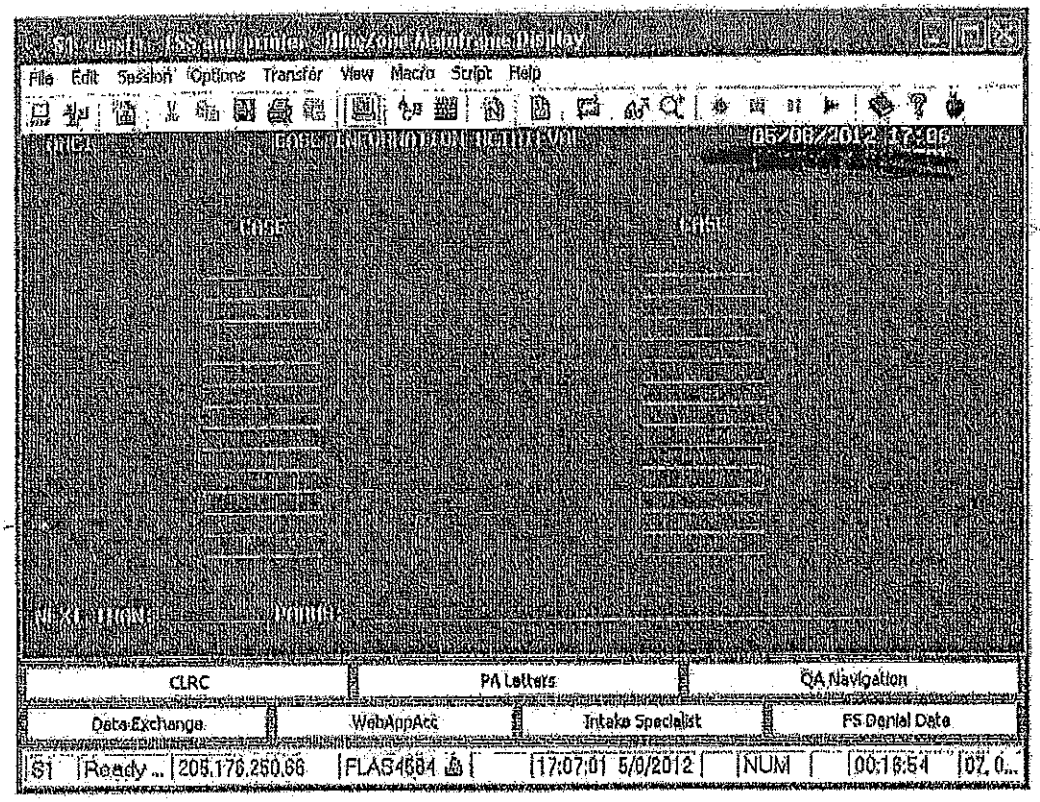


Exhibit C

FLORIDA INDIVIDUAL SECURITY INFORMATION FORM

Identifying Information:

1. _____ (Last Name) 2. _____ (First Name) 3. _____ (MI) 4. ☐ Mr. ☐ Ms. ☐ Mrs.

5. Social Security Number: _____ 6. Position Title: _____ 7. UCB: YES ☐ NO ☐

8. Agency/Business: _____ 9. Contracted with: _____ 10. Access to Federal Tax Information: YES ☐ NO ☐

10a. Access to SAVE: YES ☐ NO ☐ 10b. Access to AMS: YES ☐ NO ☐ 10c. AMS Role: _____

User ID(s) Updates: Action Required: A = ADD C = CHANGE S = SUSPEND D = DELETE R = RESTORE

11. Action Required	12. User ID	13. Worker Type	14. Security Profile Name	15. Security Level	16. Profile Begin Date	17. Profile End Date

Site Information: 18. District/CSE Region: _____ 19. Service-Site County No.: _____ 20. Service-Site Location No.: _____

21. Suncom #: _____ 22. Area Code & Phone #: _____ 23. User E-Mail Address:

FLORIDA Administrative Structure:

24. Administrative Unit Assigned: _____ 25. Supervisory Unit Assigned: _____ 26. Primary Unit Supervisor's ID: _____

27. Caseload Number: _____ 28. Supervisors Name: _____ 29. Phone #: _____

30. Justification/Comments:

☐ The employee has completed the DCF Security Awareness Training (100W) and the DCF Security Awareness Recertification Training (100BW)

☐ The employee has viewed UNAX (DOR Only)

31. _____ (Signature of Requester) _____ (Date) 32. _____ (Signature of Administrator or Next Level Supervisor) _____ (Date)

33. _____ (Signature of District/Region Security Officer) _____ (Date) 34. _____ (Signature of HQTR Security Officer) _____ (Date)

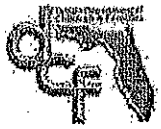
35. _____ (Signature of OPA/Program Administrator) _____ (Date)

CF 113, PDF 09/2010

Attachments: ☐ CF 114 ☐ Table Update Request ☐ Individual Contractor Security Agmnt For DOR Only: ☐ CS AT16 ☐ CS AT17 ☐ CS AT18 ☐ CS AT19 ☐ CS AT21

Exhibit C

17



SECURITY AGREEMENT FORM

The Department of Children and Families has authorized you:

_____
Employee's or Contractor'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/Contractor Name	Signature of Employee/Contractor	Date
Print Supervisor Name	Signature of Supervisor	Date

EXHIBIT D

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. 2001-64.) ([Footnote 1] Note: Repealed by s. 18, 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. 2001-64.)

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),(l)(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).

EXHIBIT D

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.

EXHIBIT D

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. 322.126 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