Attachment J: Authenticating Information and Protecting Trade Secrets

State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER: **4004**
SUBJECT: **Records Management**
DIVISION: **Operations**
BUREAU: **Support Services**
SECTION: **Records Management**

1.0 PURPOSE/SCOPE

The purpose of this policy is to provide uniform procedures for the Agency's Records Management Program. The Records Management Program exists to ensure records are maintained as appropriate, so that information is available when and where it is needed. This policy applies to all Agency employees, including OPS and contracted staff, and all Agency records regardless of the medium in which they exist.

2.0 AUTHORITY

- Chapter 119, Florida Statutes (F.S.), Public Records
- Chapter 257, F.S., Public Libraries and State Archives
- Chapter 282, F.S., Communications and Data Processing
- Chapter 501.171, F.S., Security of Confidential Personal Information
- Chapter 1B-11.004, Florida Administrative Code (F.A.C.), Use of Archives
- Chapter 1B-24, F.A.C., Public Records Scheduling and Disposition
- Chapter 1B-26, F.A.C., Records Management – Standards and Requirements
- Federal Information Processing Standards Publication Secure Hash Standards
- The Unicode Standard

3.0 DEFINITIONS

Accession - Transfer of records into the physical custody of the Department of State's State Record Center (SRC).

Active Records - Records that still have sufficient administrative, fiscal, legal, or historical value to warrant their continued storage in an easily accessible area (e.g., office area).

Archives - Inactive records which have been determined to have long term use due to their historical value.

Confidential Records - Records that the Agency is legally prohibited from making available for inspection or copying.

Disposition - Destruction of inactive records that have met their retention period.

Database - Organized collection of automated information. Chapter 1B-26.003, F.A.C. sets the standards and requirements for databases.

Database Management Systems - A set of software programs that controls the organization, storage, and retrieval of data (fields, records and files) in a database. Chapter 1B-26.003, F.A.C. sets the standards and requirements for database management systems.

DRD – The Disposition Records Document is a form used by the Department of State to request approval from the Agency to dispose of records that have met their retention schedule.

Electronic Storage - Numeric, graphic, and textual information which may be recorded in any machine readable media form which includes, but is not limited to, magnetic media, such as tapes, disks and flash drives.

Electronic Records – Any information that is recorded in machine readable form.

E-mail (Electronic Message) - A method of transmitting information that must be evaluated just like information received through mail, fax, or in person.

Exempt Records - Public records specifically exempted by law from public inspection and copying, although they may still be able to be released to the public by the Agency.

Inactive Record - Records which have lost some of their value or have been superseded by new records, but are not yet ripe for destruction. Records that are referenced less than once per month are considered inactive.

Micrographics - Area of records management associated with the feasibility, production, handling, care, and use of records which have been photographically copied and reduced in size to preserve information or reduce storage space.

Protected Health Information (PHI) - Any information, including demographic information, which relates to: the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

Public Record - Section 119.011(12), F.S., defines public records as all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

RDD – The Records Disposition Document is a form used by the Agency for records that have been stored within Agency offices and are not sent to the State Records Center for storage or disposal. The form is used to record the destruction of eligible records.

Records Custodian - Supervisor or manager in a division or bureau who has oversight authority of the records in his/her control.

Records Management Coordinator - Person designated within each Agency bureau to coordinate records management, including responses to public records requests.

Records Management Liaison Officer (RMLO) - Employee within the Bureau of Support Services assigned the responsibility of record management and quality control of records for the Agency.

Record Series – Chapter 1B-24.001(3)(k), F.A.C. defines record series as a group of related public records arranged under a single filing arrangement or kept together as a unit (physically or intellectually) because they consist of the same form, relate to the same subject or function, result from the same activity, document a specific type of transaction, or have some other relationship arising from their creation, receipt, or use. A record series might contain records in a variety of forms and formats that document a particular program, function, or activity of the agency.

Retention Schedule - Period of time in which record series are required to be retained before being scheduled for disposal.

State Records Center - Records storage facility located in Tallahassee operated by the Department of State. Also known as the SRC.

Total Recall - A web-based system which allows the user to perform certain records management functions, such as ordering supplies, accessioning items, etc., online through a secure, user specific login.

4.0 POLICY

It is the Agency's policy to ensure that public records in its custody are maintained and managed as required by Florida Public Records Law, including appropriate retention, release, and disposition. Florida Public Records Law provides that all materials made or received by Florida's state and local government agencies in connection with their official business are public records. Records may not be withheld unless the record is specifically designated under law as confidential or exempt from public disclosure.

5.0 PROCEDURES

I. Areas of Responsibility

A. The Agency has appointed a RMLO within the Bureau of Support Services. The RMLO will:

1. Ensure that all divisions comply with the requirements and procedures outlined in this policy and procedure.

2. Provide liaison between Agency Records Custodians and Coordinators and the Department of State.

3. Assist Agency staff with preparing records retention schedules, preparing records for archiving, and other records management tasks.

4. Disseminate destruction requests from the SRC as records are determined to be eligible for destruction and then submit the completed forms back to the SRC.

B. Each Bureau Chief or equivalent shall serve as the Records Custodian for all records created or received by his/her respective bureau/unit. These duties may be delegated at the discretion of the Bureau Chief, however, the Bureau Chief or equivalent retains responsibility for these records. Each Records Custodian shall:

1. Ensure security of records physically stored at his/her location;

2. Ensure proper destruction of records which have met their retention schedule and return all Disposal Request Documents (DRDs) to the Bureau of Support Services within fifteen (15) business days of receipt;

3. Ensure appropriate response to all public records requests received by his/her bureau/unit.

C. Each Bureau Chief or equivalent may also designate a Records Coordinator for his/her bureau/unit. The Records Coordinator shall:

1. Work with the RMLO to develop retention schedules as necessary;

2. Ensure that inactive records are removed from the active records inventory frequently;

3. Provide liaison between the RMLO and the Records Custodian;

4. Inform staff on changes/updates to the Agency Records Management Program;

5. Secure Records Custodian signature on DRDs for records that have met their retention schedule.

II. Records Management

A. Records management entails organization, maintenance, retention, storage, and disposition of public records.

1. Public records shall be organized, arranged, and maintained using a filing or records-keeping system that:

a. is appropriate to the nature, purpose, and use of the records;
b. can be easily understood by all users, and;
c. will facilitate the location of and access to those records, when and where it is needed.

B. Records Retention Schedules must be established for all records created and maintained by the Agency. Many of the Agency's records are covered by the General Records Schedule GS1-SL for Florida's State and Local Government Agencies (GS1-SL).

C. Any records not covered by the GS1-SL must have an individual schedule established. To establish an individual records retention schedule, contact the RMLO.

D. A link to the GS1-SL is maintained on the Bureau of Support Services' Records Management webpage.

E. Each bureau must systematically dispose of public records that have met their retention requirements and are no longer needed.

III. Inactive Records Storage (Archiving)

A. Once a record has lost its value as part of regular office operation, it is considered to be inactive. However, such records cannot be destroyed until their retention requirements have been met.

B. Inactive records may be retained in-house, imaged and stored electronically or stored in the SRC.

C. The SRC should be used to store inactive records whenever possible. If the records must be maintained in-house, they should be imaged and stored electronically if possible.

IV. Electronic Records

A. Records created or maintained in electronic format must be retained in accordance with the General Records Schedule GS1-SL (Section VI) regardless of whether the electronic records are the record copy or duplicates. A link to the GS1-SL is maintained on the Bureau of Support Services' Records Management webpage.

B. The Division of Information Technology will automatically save all non-spam filtered e-mail in archive for a period of seven (7) years. Any emails that are required to be maintained beyond that time period shall be maintained by the unit that created or received them.

C. The Agency shall develop and maintain adequate and up-to-date technical and descriptive documentation for each electronic recordkeeping system to specify characteristics necessary for reading or processing the records. The minimum documentation required is:

1. A narrative description of the system, including all inputs and outputs of the system; the organization and contents of the files and records; policies on access and use; security controls; purpose and function of the system; update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and the location and

media in which electronic records are maintained and their retention requirements to ensure appropriate disposition of records in accordance with Chapter 1B-24, F.A.C.

2. The physical and technical characteristics of the records or the equivalent information associated with a database management system including a description of the relationship between data elements in databases.

3. For information coming from geographic information systems, the physical and technical characteristics of the records must be described in a description of the graphic data structure, such as recommended by the federal Spatial Data Transfer Standards.

4. Any other technical information needed to read or process the records.

D. Electronic recordkeeping systems used by the Agency that maintain record (master) copies of public records on electronic media shall meet the following minimum requirements:

1. Provide a method for all authorized users of the system to retrieve desired records.

2. Provide an appropriate level of security to ensure the integrity of the records, in accordance with the requirements of Chapter 282, F.S.

3. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users.

4. Automated methods for integrity checking should be incorporated in all systems that generate and use official file copies of records. Hashing algorithms and digital signatures should be considered for all official file copies of electronic records. The use of automated integrity controls, such as hashing algorithms and digital signatures, can reduce the need for other security controls. Hashing algorithms used to protect the integrity of official file copies of records should meet the requirements of Federal Information Processing Standards Publication 180-4 (FIPS-PUB 180-4) entitled "Secure Hash Standard". Agencies utilizing hashing algorithms shall only use validated implementations of hashing algorithms.

5. Identify the open format or standard interchange format when necessary to permit the exchange of records on electronic media between Agency electronic recordkeeping systems using different software/operating systems and the conversion or migration of records on electronic media from one system to another. For text records in the absence of other conversion capabilities, the word processing or text creation system should be able to import and export files in the ASCII or Unicode format as prescribed by the Unicode 5.0 Standard (or successor Unicode Standard).

6. Provide for the disposition of the records including, when appropriate, transfer to the SRC.

7. E-mail is not an appropriate storage media for documents to be retained. If a document requires retention, the document should be saved from e-mail to an approved format and system for retention. (For example Laserfiche or Sharepoint).

8. See also Email Retention Policy 5004.

V. Records Destruction

A. Records stored at the State Records Center

1. Twice a year the Department of State provides the RMLO with a list of documents, which have met their retention requirements and are eligible for destruction.

2. The RMLO will distribute the Disposition Request Documents (DRDs) to the appropriate Records Custodian for signature.

3. Unless the records are related to pending litigation, the DRDs should be signed and returned to the Agency RMLO for processing within fifteen (15) business days of receipt.

4. The RMLO will return the DRDs to the Department of State, and then the records will be destroyed.

B. Records stored within Agency Facilities

1. Identify records which have met their retention requirements and are eligible for destruction.

2. The completed Records Disposition Documents (RDDs) should be signed and returned to the Agency RMLO.

3. Identify documents that contain, or may contain confidential information or Protected Health Information (PHI) that are ready for disposal.

4. Place the identified documents in a locked shred bin.

5. If a locked shred bin is not available, or they are full, store the PHI in a locking file cabinet or a locking office until such time as an empty locked shred bin is available. Locking, rolling shred bins may also be available from your field office shredding contractor to handle overflow situations.

6. Never place PHI in regular trash or recycle bins – it must always be shredded.

7. If you are aware of PHI having been placed in regular trash, retrieve the PHI and properly dispose of it by shredding or placing it in a locked shred bin. If it is not possible to retrieve the PHI (for example, it has made it all the way to a dumpster), secure the trash receptacle/dumpster by posting staff near it to

deter access/emptying. Immediately, by direct telephone contact, contact the Agency HIPAA Privacy Officer and the facility management representative.

8. If you are unsure that something is, or contains PHI, shred it.

C. Records stored electronically

Electronic records may be destroyed only in accordance with the provision of Chapter 1B-24, F.A.C. Minimum standards are described in Chapter 1B-26.003, F.A.C. The Agency's Information Technology (IT) policy on media destruction (#08-IT-05) and Agency HIPAA policy (#4031), also discuss destruction of confidential electronic records.

In accordance with Section 501.171 (8), F.S., enacted in 2014, the Agency qualifies as a covered entity. The requirements from Section 501.171, F.S., is as follows: (8) REQUIREMENTS FOR DISPOSAL OF CUSTOMER RECORDS.—Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee and contracted vendor to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions.

8.0 REVISION HISTORY

Author: Brian Kenyon **Date:** October 1, 2014

Approved by: Tonya Kidd **Date:** November 3, 2014

1st Revision Approved by: Tonya Kidd **Date:** January 20, 2016

2nd Revision Approved by: Jon Manalo **Date:** June 14, 2019

Deletion Approved by: _____ **Date:** _____

9.0 ATTACHMENT(S)

State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER: **4029**
SUBJECT: **Security and Identification Badges**
DIVISION: **Operations**
BUREAU: **General Services**
SECTION: **Facilities Management**

1.0 PURPOSE/SCOPE

To provide maximum safety and security for individuals and facilities, through the use of identification badges/access cards, limiting access to Agency facilities, and following proper security policies and procedures.

2.0 AUTHORITY

Section 20.05(1)(b), Florida Statutes, provides that the head of a department may delegate to administrative units, assistants and deputies any power, duty or function not explicitly required by law to be performed without delegation.

3.0 DEFINITIONS

Access Card – A plastic card that contains a Radio-frequency Identification (RFID) chip for encrypted data that is read by passing the card through, over or in front of a corresponding electronic device, to gain access to a restricted or secured area.

Access Code – A sequence of characters that allows user access to a secure area.

Home Building – In security scenarios, refers to the specific building in which a person's office is located rather than an entire office complex.

Identification (ID) Badge - Issued to Agency employees and Agency contracted employees, consultants and vendors who may need to show proof of representing the Agency. The ID badge displays a photo of the individual along with their name, bureau/unit, position title and Agency logo. ID badges are used to gain entry to Agency buildings and offices.

Piggybacking – In security scenarios, when an authorized person allows someone to follow through a door to a secure area. Unlike tailgating, piggybacking is intentionally allowing an individual to circumvent security measures.

Tailgating – In security scenarios, when a person follows someone or is waiting in close proximity to a door and is able to access the door before it closes and then proceeds in to gain entry to restricted or secure area.

Security – Procedures followed or measures taken to help ensure the safety of the Agency. Security is the responsibility of every individual.

Temporary Access Card – Issued to Agency employees, consultants and vendors in Tallahassee for one (1) day use to gain entry to Headquarters buildings and offices.

Visitor Badge – A temporary numbered ID badge issued for purposes of identity only. A visitor's badge does not grant access to any facility via card readers.

Visitor Sign-in Log – A log of all visitors to a facility that contains at a minimum the following information: date of visit; visitor badge number; printed name of visitor; signature of visitor; Agency contact person/office; the name of the individual that escorts the visitor; visitor time in; and visitor time out.

4.0 POLICY

All employees, consultants and vendors are required to comply with all security policies and procedures. Every supervisor is responsible for ensuring that all of their employees become familiar with all security procedures. Failure to do so jeopardizes not only individual safety, but also the safety of others, and the information the Agency safeguards.

This policy is prepared for all Agency offices, including field office facilities. Field offices may have additional security procedures in place for its facility. This policy serves as additional direction and a supplemental resource to those facility unique procedures.

5.0 PROCEDURES

I. General Facility Security

A. Facility Access

1. Access to Agency facilities is restricted twenty-four (24) hours a day, seven (7) days a week to Agency employees, persons providing contract services, vendors performing services and visitors who have business at Agency facilities.

2. Except for Executive Management, actual 24/7 access privileges shall be restricted to an employee's home building.

3. Temporary ID badges/access cards can be issued as appropriate for access, but will be time limited.

4. It is the responsibility of the Bureau of General Services, working with management at the Headquarters complex and field offices to identify necessary access controls in all Agency facilities.

5. Accessibility to confidential/sensitive information may necessitate restricted access to certain areas.

6. Upon termination or transfer of an employee, consultant or vendor, it is the immediate supervisor's responsibility to obtain and return the ID badge/access card to the Bureau of General Services, or the Field Office Management in the Field Office.

B. Obtaining an ID Badge/Access Card

1. Headquarters

a. Complete the HQ Identification/Security Badge Request Form. This form may be obtained from the Bureau of General Services Portal Page under Facilities Management. The original completed form must be received by the Bureau of General Services before an ID badge/access card will be issued.

b. This form must be approved by the supervisor and bureau chief or higher authority.

c. Employees, consultants and vendors must contact the Bureau of General Services at 850-412-3888 or Facilities_Requests@ahca.myflorida.com to make an appointment for an ID badge/access card.

d. Photographs are taken and ID badges/access cards are issued on normal business days between 9:00 a.m. and 4:00 p.m. in Fort Knox Building 2, Room 203-P.

e. Employees, consultants and vendors shall bring a valid State-issued ID to the appointment in order to receive an ID badge/access card.

2. Field Offices

The field office appointed liaison will take the picture and email it to the Bureau of General Services at Facilities_Requests@ahca.myflorida.com, along with the completed Field Office Photo Identification Badge Request Form. The ID badge will be sent to the appointed liaison for distribution.

3. Issuance of ID badges/access cards shall be controlled. The Bureau of General Services maintains a log identifying when and to whom ID badges/access cards are issued. Field office supervisors maintain a log for their ID badges/access cards.

4. Upon the termination or transfer of an employee, consultant or vendor, it is the immediate supervisor's responsibility to obtain and return the ID badge/access card to the Bureau of General Services, or the supervisor responsible for security in the field office.

5. Any person suspecting that an ID badge/access card has been lost or stolen shall immediately notify their supervisor. The supervisor shall then notify the Bureau of General Services or the field office management or designee to begin precautionary security measures.

Limiting Access

1. The security guard/receptionist shall not allow any individual into an Agency facility who does not have a valid Agency ID badge/access card.

2. The ID badge/access card shall be prominently displayed at all times by all individuals while in a facility. If the photo on an ID badge is damaged, the employee, consultant or vendor shall request a new ID badge.

3. All visitors shall be escorted to and from all destinations while in a facility. A visitor's badge is for identity only, and does not grant access to any facility.

4. All employees, consultants and vendors shall use their ID badge/access card to gain entry to buildings and offices.

5. Employees, consultants and vendors shall not allow anyone access (e.g., to follow them through a doorway) to any building or office.

6. Anyone without an ID badge/access card, attempting to tailgate, shall be directed or escorted depending on the circumstances to the receptionist at the main entrance of the building or office suite to sign in and secure a visitor's badge and then escorted to their business location. If the person does not comply, the situation should not become confrontational. Instead, building security should be notified or 911 should be called immediately as appropriate.

7. Employees shall not loan or borrow another employee's ID badge/access card to circumvent security access points.

8. Employees shall not allow anyone access to Agency offices on nights and/or weekends to anyone who does not have 24/7 access.

C. Conferences, Group Meetings and Trainings

1. If visitors are to attend a scheduled group meeting, conference, or training, the security guard/receptionist will ask for the location of the meeting and the name of the meeting coordinator.

2. The meeting coordinator shall be prepared to meet all visitors at the security/receptionist desk prior to the scheduled meeting start time.

3. The meeting coordinator is responsible for expediting sign in and ensuring that visitors are provided directions to the appropriate conference room.

4. After the meeting or conference is over, the meeting coordinator is responsible for signing out visitors and collecting the visitors' badges.

II. Headquarters (Fort Knox Office Complex) Security and Access

A. Security Guard/Escort Service

1. Uniformed security guards are on duty Monday through Friday, except for observed State holidays. Two (2) uniformed security guards are on duty between the hours of 7:00 a.m. and 5:00 p.m. and One (1) uniformed security guard will be on duty, until 8:00 p.m. One (1) security guard will be located at the security station in the lobby area of Building 3, from 7:30 a.m. to 5:30 p.m. and the second security guard will patrol the complex and relieve the Building 3 security guard as necessary.

2. The security guards may be contacted by telephone at 850-412-3913 (desk), or 850-661-4487 (cellular).

3. Employees can request an escort to their vehicle after 5:00 p.m. up until 7:45 p.m., Monday through Friday, excluding state holidays or state mandated closings. Employees should call security at least fifteen (15) minutes prior to their desired departure time.

4. If an individual experiences or witnesses an event that should be reported, they should call 911 or the Bureau of General Services to report the event as appropriate.

5. Security guards shall notify General Services by phone of any issues concerning the Agency's physical security.

6. General Services will maintain a log of security issues and General Services responses.

B. Access Control

1. Access to the Fort Knox Office Complex is controlled through the use of electronic card readers and ID badges/access cards. The readers are located at the main entrance of each building and/or suite.

2. The security guard stationed in the lobby area of Building 3 controls access and assists employees, consultants, vendors and visitors with security issues.

3. A roving security guard is also on property to assist employees, consultants, vendors and visitors with security issues and relieve the security guard stationed in Building 3 as necessary.

4. The receptionists located within Building 2 control access to their respective suites in the building. The building is accessible by employees, consultants and vendors with an ID badge/access card.

5. Management at the bureau chief level or above is responsible for reviewing the security access needs for their employees, consultants and vendors.

6. Access request change(s) shall be sent to the Bureau of General Services, who will coordinate with the requestor to make the appropriate changes.

7. Access to buildings outside of normal business hours should be restricted to necessary staff with ID badges/access cards.

8. Employees on the Fort Knox Office Complex campus outside of normal working hours may be asked to present their Agency ID Badge and also a state issued ID (in addition to their Agency ID Badge) for verification purposes. Employees unable to provide both forms of identification will be instructed to leave and escorted off property.

9. Issuance of permanent ID badges/access cards is limited to employees, consultants and vendors who frequently provide services within the Fort Knox Office Complex. Consultants and vendors will be assigned an ID badge/access card at the discretion of the respective bureau chief. All other consultants and vendors will be assigned a visitor's badge to be used while they are in the building.

10. Access to the Computer Resource Center (CRC) is restricted. General Services will provide a report each month to the IT Security Office of all physical access to the CRC via access card logs. General Services will also provide a list of all card holders with access to the CRC to the IT Security Office for review.

11. General Services shall perform monthly reviews of security camera footage.

12. General Services shall perform an annual review of the access cards permissions for each bureau at Headquarters. The bureau chiefs will be required to respond with approval or any changes necessary.

13. Supervisors at Fort Knox Office Complex may request employee, consultant or vendor access reports from the Bureau of General Services.

a. All employee, consultant or vendor access report requests require the approval of the appropriate bureau chief.

b. All badge report requests should be emailed to Facilities_Requests@ahca.myflorida.com.

C. Visitor Badges

1. All visitors shall be issued a visitor's badge. Visitor badges have no access privileges through the card readers in the facilities. All visitor's will be required to provide a state issued ID before a visitor's badge is issued.

2. The security guard located at the security station in the lobby area of Building 3 shall be responsible for issuing visitor badges for Building 3.

3. The receptionists located within Building 2 shall be responsible for issuing visitor badges for their respective offices.

4. Issuance of visitor badges requires the security guard/receptionist greet visitors; issue visitor badges; and maintain a Visitor's Sign-In Log, ensuring that all required information has been entered prior to providing a visitor's badge.

5. General Services shall perform a monthly review of all visitor logs.

D. Temporary Access Cards

1. Employees, consultants and vendors must contact the Bureau of General Services at 412-3888 or Facilities_Requests@ahca.myflorida.com to make an appointment for a temporary access card.

2. Employees, consultants and vendors must bring a valid State-issued picture ID to the appointment in order to receive a temporary access card.

3. A temporary access card will be activated for one (1) day for the employee, consultant or vendor's assigned building from 8:00 a.m. to 5:00 p.m.

4. The temporary access card must be returned to the Bureau of General Services by 5:00 p.m. on the day it is issued or at the beginning of the following business day.

5. The temporary access card shall be prominently displayed at all times while in a facility.

6. Employees, consultants and vendors may be asked by security to verify their identity when walking through the facilities while wearing a temporary access card.

7. When entering Building 3, an employee, consultant or vendor wearing a temporary access card shall present a valid State-issued picture ID to the security officer(s) at the security desk in order to verify identity.

8. Employees, consultants and vendors may be charged for the cost of a replacement card if the temporary access card is not returned within two (2) business days of issuance.

E. Replacement of ID Badge/Access Cards

1. Employees, consultants and vendors must complete the HQ Identification/Security Badge Request Form. The form may be obtained from the Bureau of General Services Portal Page under Facilities Management . The original completed form must be received by the Bureau of General Services before a replacement ID badge/access card will be issued.

2. The form must be approved by the supervisor and bureau chief or higher authority.

3. Employees, consultants and vendors must contact the Bureau of General Services at 850-412-3888 or Facilities_Requests@ahca.myflorida.com to make an appointment for a replacement ID badge/access card.

4. Photographs are taken and ID badges/access cards are issued on normal business days between 9:00 a.m. and 4:00 p.m. in Ft. Knox Building 2, Room 203-P.

5. Employees, consultants and vendors shall bring a valid State-issued ID to the appointment in order to receive a replacement ID badge/access card.

6. Employees, consultants and vendors may be charged for the cost of a replacement ID badge/access card.

7. If an employee with 24/7 access privileges loses their access card two times in two calendar years requiring the issuance of permanent replacement access cards, that employee shall forfeit their 24/7 access.

8. Employees, consultants and vendors are to have only one ID badge/access card. If an employee, consultant or vendor is issued a replacement ID badge/access card and the "lost" ID badge/access card is later found, the employee, consultant or vendor must return the "lost" ID badge/access card to the Bureau of General Services. The "lost" ID badge/access card will not be re-activated.

9. Employees suspecting that an ID badge/access card has been lost or stolen shall immediately notify their supervisor. The supervisor shall then notify the Bureau of General Services or the field office management or designee to begin precautionary security measures.

III. Field Office Security and Access

A. Each field office has security procedures in place for its facility. The security varies depending on location and building management; however, all offices are secured twenty-four (24) hours a day, seven (7) days a week through the use of electronic coded keypads, electronic security access systems or manual locks used to control access to the building and/or suite.

B. The Field Office Management or their designee is responsible for coordinating and/or maintaining the security system in their facility and controlling issuance of ID badges/access cards and codes for accessing the facility.

C. Whenever an employee, consultant or vendor terminates or transfers, it is the supervisor's responsibility to obtain the ID badge/access card and/or reset the access code.

D. The access code should be changed periodically. Whenever an access control system code is changed, all affected employees, consultants and vendors should be notified.

E. General Services will annually survey and ask for an attestation from the Field Office Management stating that the Field Office is following the procedures listed in Agency Policy 4029.

F. General Services will annually survey and ask for an attestation from the Field Office Management stating that the Field Office has performed an annual review of employee access permissions and that any necessary changes have been made.

G. Temporary Access for misplaced ID badges

Any employee, consultant or vendor who misplaces their ID badge/access card shall secure a visitor's badge from the security guard/receptionist or their field supervisor or designee and return it at the end of the business day.

H. Replacement of ID Badge/Access Cards

1. The Bureau of General Services or the field office supervisor shall be contacted for a replacement ID badge/access card.

2. The field office appointed liaison will take the picture and email it to the Bureau of General Services at Facilities_Requests@ahca.myflorida.com, along with the

completed Field Office Photo Identification Badge Request Form. The ID badge/access card will be sent to the appointed liaison for distribution.

3. Employees, consultants and vendors may be charged for the cost of a replacement ID badge/access card.

4. If an employee with 24/7 access privileges loses their access card two times in two calendar years requiring the issuance of permanent replacement access cards, that employee shall forfeit their 24/7 access.

5. Employees, consultants and vendors are to have only one ID badge/access card. If an employee, consultant or vendor is issued a replacement ID badge/access card and the "lost" ID badge/access card is later found, the employee, consultant or vendor must return the "lost" ID badge/access card to the Bureau of General Services. The "lost" ID badge/access card will not be re-activated.

6. Employees suspecting that an ID badge/access card has been lost or stolen shall immediately notify their supervisor. The supervisor shall then notify the Bureau of General Services or the field office supervisor or designee to begin precautionary security measures.

7. General Services shall perform annual reviews to ensure that Field Offices are following the appropriate safety and security measures.

IV. Physical Security

A. All employees, consultants and vendors are required to use their ID badge/access card to gain access to a facility.

B. Doors designated to be locked shall be kept locked at all times. Doors must not be propped open if they should be locked. This reduces the overall security of the building.

C. If a visitor is found to be in a facility without proper authorization, they shall be asked to leave and escorted to the main entrance. If they have legitimate business in the facility, they may secure a visitor's badge and the person they are there to see will be called to escort them. **Under no circumstances shall Agency employees, consultants or vendors enter into a verbal or physical confrontation with a visitor.** If the visitor at any point becomes uncooperative or refuses to leave, building security or 911 shall be called as appropriate.

D. Any problems noted with any part of the security system shall immediately be reported to the Bureau of General Services and the Field Office Manager as appropriate.

E. Other problems noted, such as doors propped open that should be closed or doors unlocked which are designated to be locked, may be corrected by the employee, consultant or vendor. The issue should then be reported to the Bureau of General Services and the Field Office Manager as appropriate.

F. Public meetings shall only be scheduled to begin and end during business hours. For purposes of this policy, business hours are Monday through Friday, 8:00 AM to 5:00 PM. Public meetings shall end with enough time for the public to sign out, return their visitor badges, and be escorted or otherwise certified to have left the building no later than 5:00 PM by Security.

G. If a former employee requests to pick up personal property that was left in Agency office space, the supervisor must provide all of the pertinent information to the Bureau of General Services or field office management as appropriate in order for the process to be coordinated with as little disruption to normal operations a as possible.

1. Arrangements for the pick-up of personal property will be made by the Bureau of General Services or field office management as appropriate based on the following parameters:

a. Safety and security of Agency personnel and facilities;
b. Size and amount of items to be picked-up; and
c. Availability of staff and/or security guards to meet the former employee.

2. If a former employee does not make arrangements to retrieve their personal property within thirty calendar days of the last date of employment, the property will be disposed of as appropriate.

3. Refer to the Agency Property Management Policy 4007 – Section VI., Personal Property.

V. Personal Security Recommendations

A. Personal Security

In order to reduce the risk of loss, it is recommended that personal valuables such as purses, wallets, etc. be secured in a locked drawer when left unattended. It is recommended that employees, consultants and vendors refrain from bringing personal valuables into the office.

B. Parking

If an employee, consultant or vendor is on-site after normal working hours, it is recommended that the employee, consultant or vendor move their car as close to the main entrance as possible and park in a well-illuminated and secure location.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions.

8.0 REVISION HISTORY

Author: Jennifer Barrett **Date:** April 14, 2014

Approved by: Tonya Kidd **Date:** April 21, 2014

1st Revision Approved by: Tonya Kidd **Date:** November 3, 2014

2nd Revision Approved by: Tonya Kidd **Date:** February 16, 2016

3rd Revision Approved by: Tonya Kidd **Date:** January 27, 2017

4th Revision Approved by: Julie Madden **Date:** May 17, 2022

9.0 ATTACHMENT(S)

HQ Identification/Security Badge Request Form, AHCA FORM 2200-4004 (JAN-22)
Field Office Photo Identification Badge Request Form, AHCA FORM 2200-4100 (JAN-22)

HQ IDENTIFICATION/SECURITY BADGE REQUEST FORM

ID Card Production Service by Appointment Only
Monday thru Friday 9 AM - 12 PM and 1 PM - 4 PM

Name: _____ Employee Type: _____
(Employee, Vendor, Intern ETC.)

Title: _____ HQ Building #: _____

New Issue: ☐ Access Modification: ☐

Bureau: _____ Replacement Issue: ☐ Name Change: ☐

Access Request for Building: _____ Requested Access: _____

NOTE: MONDAY - FRIDAY IS FROM 6:45 am - 6:15 pm ONLY

SPECIAL BUREAU / UNIT ACCESS AUTHORIZATION

Bureau/Unit Access: _____

Bureau Chief: _____ Signature: _____
(Print Name)

Authorization Signature: _____
(Area Office Supervisor, Bureau Chief or Higher)

Supervisor Signature: _____

This identification/security access card is **STATE PROPERTY.** By receipt of this card, the recipient agrees to:

1. Notify General Services at 412-3888 **IMMEDIATELY** of a lost or stolen card. Initial: ____
2. Assume responsibility to safeguard and secure the card from damage, theft, or misuse. Initial: ____
3. Return card upon termination or request. **NOTE:** Access can be denied without prior notification. Initial: ____

This ID badge/access card shall be prominently displayed at all times while in the **AGENCY** facilities. Employees, consultants, and vendors shall not allow **ANYONE** without a visible ID badge/access card to enter any secured building or office suite (aka **"TAILGATE"**). Headquarters employees who have not worn their ID badge should report to **GENERAL SERVICES** to be issued a **TEMPORARY ACCESS CARD.**

Employee Signature: _____ Date: _____

BUREAU OF GENERAL SERVICES USE ONLY

Card Number: _____ Date Issued: _____

FIELD OFFICE PHOTO IDENTIFICATION BADGE REQUEST FORM

Name: _____ Employee Type: _____
(Employee, Vendor, Intern ETC.)

Title: _____ City: _____

Bureau: _____ New Issue: ☐ Access Modification: ☐
Replacement Issue: ☐ Name Change: ☐

Authorization Signature: _____
(Area Office Supervisor, Bureau Chief or Higher)

Supervisor Signature: _____

This identification/security access card is **STATE PROPERTY.** By receipt of this card, the recipient agrees to:

1. Notify Field Office Management **IMMEDIATELY** of a lost or stolen Access card. Initial: ____
2. Notify General Services at 412-3888 **IMMEDIATELY** of a lost or stolen photo ID. Initial: ____
3. Assume responsibility to safeguard and secure the card from damage, theft, or misuse. Initial: ____
4. Return card upon termination or request. **NOTE:** Access can be denied without prior notification. Initial: ____

This ID badge/access card shall be prominently displayed at all times while in the **AGENCY** facilities. Employees, consultants, and vendors shall not allow **ANYONE** without a visible ID badge/access card to enter any secured building or office suite (aka **"TAILGATE"**). Headquarters employees who have not worn their ID badge should report to **GENERAL SERVICES** to be issued a **TEMPORARY ACCESS CARD.**

Employee Signature: _____ Date: _____

BUREAU OF GENERAL SERVICES USE ONLY

Card Number: _____ Date Issued: _____

Agency for Health Care Administration

HIPAA/HITECH

Policies and Procedures Manual

Attachment to: AGENCY POLICY #4031
Revision Date: 07/02/2020

Table of Contents

Introduction

This manual describes the privacy law under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology Economic and Clinical Health (HITECH) Act, Federal Medicaid law and the Agency's procedures for complying with the law.

The policies and procedures contained in this manual are applicable to all members of the Agency's workforce (workers). The terms "Agency workforce" and "Agency worker" as used in this manual encompass Agency employees, volunteers, trainees, student interns, and other persons who work for the Agency in the capacity of contracted staff or consultants under the direct control of the Agency.

Generally, each topic section of this manual is divided into two parts: (1) a summary of the law and (2) an explanation of the Agency's procedures for complying with the law. Some topics may have only a "law" section, and some may have only a "procedure" section.

Please note that the "law" sections are summaries, paraphrases, or interpretations of the law, and not the precise language of the law itself. The summaries may not include all of the requirements of the law, just the applicable ones. If you have any questions about the requirements of the privacy law or should any conflicts between this manual and the law itself arise, contact the Agency's HIPAA Privacy Officer or the General Counsel's Office.

Health Insurance Portability and Accountability Act (HIPAA)

45 CFR Parts 160, 162 and 164

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). Among other purposes, HIPAA increases the "accountability" of those who handle health information by:

- Limiting the use and disclosure of protected health information;
- Requiring each covered entity to develop reasonable safeguards to protect the privacy of health information;
- Imposing civil and criminal penalties for the improper use or disclosure of protected health information; and
- Providing greater rights for people to obtain access to their health information.

The Privacy Rule contains specific provisions for the use and disclosure of Protected Health Information (PHI). All covered entities, which includes health care providers, health plans (including Medicaid) and health care clearinghouses, are required to comply with the provisions of the Privacy Rule, which went into effect on April 14, 2003.

For the complete text of the HIPAA Privacy and Security Rule, see the Health and Human Services

(HHS) Office for Civil Rights website at http://www.hhs.gov/ocr/privacy. You can also request a paper copy from the HIPAA Privacy Officer
.

Health Information Technology Economic and Clinical Health (HITECH) Act

Title XIII of Division A and Title IV of Division B of the
American Recovery and Reinvestment Act of 2009 (ARRA) (Public Law 111–5)

In 2009, Congress passed the Health Information Technology Economic and Clinical Health (HITECH) Act. Among other purposes, HITECH increases the accountability of those who handle health information by:

- Increasing the civil monetary penalties for those who disclose health information in an unauthorized manner from up to $25,000 per incident under HIPAA to up to $1,500,000 per incident under HITECH;
- Requiring business associates that handle PHI on behalf of an agency to also comply with the Privacy Rules as though they were a HIPAA covered entity;
- Requiring that a public media announcement be published, conspicuous notice on a public web site, or notifications be sent to persons whose health information has been disclosed in an unauthorized manner if the information was not either encrypted or destroyed;
- Requiring that all health data stored in an Electronic Health Record (EHR) system be tracked if the patient requests an accounting of disclosures, including those for treatment, payment or health care operations; and
- Prohibiting the sale of health data stored in an EHR

Omnibus HIPAA Final Rule of 2013

The final rule implementing and revising various provisions of HIPAA/HITECH was published in the Federal Register January 25, 2013. These modifications, collectively referred to as the Omnibus HIPAA Final Rule, were effective March 26, 2013 with full compliance by covered entities and business associates required by September 23, 2013.

In summary, key changes include: expansion of the definition of a business associate; the requirement that business associates and subcontractors comply with certain aspects of HIPAA/HITECH and are directly liable for non-compliance; limitation on the use and disclosure of PHI for marketing and fundraising purposes; prohibition on the sale of protected health information without individual authorization; prohibition on health plans using or disclosing genetic information for underwriting purposes; allowance for covered entities to provide PHI to family members or friends of decedents who were involved with the decedent's care; requirement for Notice of Privacy Practices modifications and redistribution of those notices; adoption of a new breach notification standard wherein covered entities must perform a four-factor breach risk assessment in the event of an unauthorized PHI disclosure.

The breach risk assessment is conducted by the Agency's HIPAA Privacy Officer. Any worker who has knowledge that an unauthorized disclosure of PHI may have occurred should immediately

notify the work unit supervisor and the Agency's HIPAA Privacy Officer.

Federal Medicaid Regulations

42 U.S.C. 1396(a)(7)

The federal Medicaid regulations that safeguard Medicaid information have been in effect since 1979. **The Medicaid regulations restrict the use and disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the Medicaid State Plan**. For the complete text of the Medicaid regulations, see Title 42 CFR, Part 431, Subpart F and Subpart G, on the National Archives and Administration Website at https://www.govinfo.gov/app/collection/cfr/2018/title42/chapterIV/. You can also request a paper copy from the HIPAA Privacy Officer.

When Regulations Differ

45 CFR 160.202

Some of the provisions of the HIPAA Privacy Rule differ from Medicaid and other state and federal regulations. Personnel should be very careful when using or disclosing Medicaid recipient information. **There are many situations where a particular use or disclosure of health information may be permitted under HIPAA, but is not permitted by Medicaid law.**

If you have any questions regarding which regulation applies in a given situation, you should refer the situation to the Agency HIPAA Privacy Officer before using or disclosing any protected health information.

Chapter One:
Use and Disclosure of Protected Health Information (PHI)

This chapter focuses on how to identify Protected Health Information and understanding when protected health information may be lawfully used and disclosed. This chapter is divided into six sections:

A. General Rules
B. When an Authorization is Not Required
C. When an Authorization Is Required
D. When an Individual Must Be Given an Opportunity to Agree or Object
E. De-Identification and Limited Data Sets
F. Improper Use and Disclosure

A. General Rules

The following are general rules for using and disclosing protected health information, including: (1) how to recognize protected health information and what information is protected under Medicaid law; (2) uses and disclosures for treatment, payment, and health care operations; (3) the Minimum Necessary Standard; and (4) verification of identity.

1. Recognizing Protected Health Information

45 CFR 164.502(a)
45 CFR 164.501
45 CFR 160.102
45 CFR 160.103
45 CFR 164.502(f)

Use and Disclosure Under HIPAA

The Agency may not use or disclose Protected Health Information (PHI) except as permitted by the HIPAA Privacy Rule. The Agency must comply with the use and disclosure requirements with respect to the PHI of a deceased individual for a period of 50 years following the death of the individual.

Definition of Protected Health Information

Protected Health Information is individually identifiable health information about:

a) A person's physical or mental health or condition; or
b) The provision of health care to a person; or
c) The payment for the provision of health care to a person;

and

The information identifies the person, or can reasonably be used to identify the person. *For example*: *a medical record that states, "Patient John Doe has the measles." The record describes John Doe's health condition and identifies him by name; therefore, it contains PHI.*

Examples of Identifiers

45 CFR 164.514(b)(2)

Identifying data (also known as "an identifier") is data that could reasonably be used to identify a person. Please note that identifiers include data that directly identifies the individual, as well as any relatives, employers, or household members.

For example: an insurance document that has my name blacked out, but lists my employer's name would still be PHI, because someone could reasonably use my employer's name to identify me.

The following are examples of identifiers and must be redacted in order for information to be de-identified under the HIPAA Safe Harbor Method of de-identification (see also Chapter 1, E. 1., "De-identification":

a) Names;
b) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes;
c) All elements of dates (except year) directly related to an individual, including birth date, admission date, date of service, discharge date, and date of death (the birth year of individuals age 90 and over is also an identifier).
d) Telephone numbers;
e) Fax numbers;
f) Electronic mail addresses;
g) Social security numbers;
h) Medical record numbers;
i) Health plan recipient numbers;
j) Account numbers;
k) Certificate/license numbers;
l) Vehicle identifiers and serial numbers, including license plate numbers;
m) Device identifiers and serial numbers;
n) Web Universal Resource Locators (URLs);
o) Internet Protocol (IP) address numbers;
p) Biometric identifiers, including fingerprints, and voice prints;
q) Full face photographic images and any comparable images;
r) Any other unique identifying number, characteristic or code; and
s) The Agency does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

PHI Can Be in Any Form of Communication or Media

PHI includes written, electronic, and oral communications.

For example: email, fax, online databases, voice mail, a photograph, a video/audio recording, or a conversation.

Past, Present and Future

PHI relates to an individual's past, present or future health condition, health care, or the payment for health care.

Exclusions

42 USC 1396a

Some types of health information are excluded from being considered PHI even if they can be used to identify the individual. The exclusions are:

a) Education records covered by the Family Educational Rights and Privacy Act (FERPA);
b) Student health records (age 18 or over) maintained by a health care provider who is treating the student; and
c) Employment records held by a covered entity in its role as employer.

Medicaid Information

42 CFR 431.302
42 CFR 431.305

Apart from the requirements of HIPAA, **federal Medicaid regulations restrict the use and disclosure of information concerning Medicaid program applicants and recipients to purposes directly connected with the administration of the Medicaid State Plan**. These purposes include:

a) Establishing eligibility;
b) Determining the amount of medical assistance;
c) Providing services to recipients; and,
d) Conducting or assisting an investigation, prosecution, or civil or criminal proceeding relating to the administration of the Medicaid State Plan.

Information about Medicaid applicants and recipients that must be safeguarded from improper use and disclosure includes:

a) Names and addresses;
b) Medical services provided;
c) Social and economic conditions or circumstances;

d) Agency evaluation of personal information;
e) Medical data, including diagnosis and past history of disease or disability;
f) Any information received for verifying income eligibility and amount of medical assistance payments; and
g) Any information received in connection with the identification of legally liable third party resources.

Workers using or disclosing Medicaid recipient information are required to follow the requirements of both HIPAA and Medicaid law. Regardless of HIPAA, **information about Medicaid recipients may only be disclosed for purposes directly connected with administering the Medicaid State Plan.**

If you are uncertain whether a particular use or disclosure of PHI is permitted under HIPAA or Medicaid law, consult with your supervisor, the General Counsel's Office or the HIPAA Privacy Officer prior to using or disclosing the information.

2. Treatment, Payment, and Health Care Operations (TPO)

45 CFR 164.502(a)
45 CFR 164.506

The Agency is permitted to use or disclose PHI for **treatment, payment,** and **health care operations**.

See Appendix "A" – Glossary for the full definition of the terms "Treatment," "Payment," and "Health Care Operations."

Treatment

The Agency does not provide direct treatment to recipients. However, Child Health Check-Up reminder letters and field office Child Health Check-Up referrals are considered treatment activities under HIPAA regulations. Medicaid may disclose PHI to an applicant's or recipient's treating provider to enable the applicant/recipient to receive health care.

Payment

The Agency's payment activities include, but are not limited to:

a) Eligibility verification
b) Billing and claims processing
c) Medical review, utilization review, and pre-certification and pre-authorization of services

Examples of these activities are listed below.

a) Eligibility Verification

The Agency may use or disclose PHI for eligibility verification functions. Examples are:

- Eligibility determinations by the Department of Children and Families (DCF). DCF determines eligibility for low-income families; pregnant women; children in foster care; special-needs adoptee; elderly, blind and disabled adults; and individuals in need of hospice or institutional care
- Presumptively eligible pregnant women eligibility determinations by the Department of Health, Regional Perinatal Intensive Care Centers, and other qualified providers
- KidCare eligibility determinations by the Florida Healthy Kids Corp.
- Data exchange with the Social Security Administration to identify Social Security Income recipients and perform Medicare buy-in activities for dual eligible recipients
- Resolutions of enrollment errors by Medicaid staff
- Production of Medicaid identification cards by the Medicaid fiscal agent or its subcontractor
- Managed care enrollment activities by a private contractor to assign recipients to a managed care entity
- Provision of enrollment, dis-enrollment, and error lists to Medicaid's managed care entities, e.g., Health Maintenance Organizations (HMO) and Provider Service Networks (PSN)
- Medicaid Eligibility Verification Services (MEVS) provided by private contractors for providers to verify recipients' eligibility, managed care assignment, coverage type, and service limits
- Data exchange with the Internal Revenue Service to verify recipient income and assets for eligibility determinations

b) Billing

The Agency may use and disclose PHI for billing functions. Examples are:

- Claims management by the Medicaid fiscal agent
- Claims resolution by the Medicaid Claims Resolution Unit and field office staff to adjudicate claims that have exceeded the time limit, for out-of-state services, or have other problems
- Claims processing and payment for certain services by AHCA Finance and Accounting
- Pursuit of third party liability (TPL) payments by Medicaid workforce members and the TPL contractor
- Journal transfers from AHCA to other state agencies to reimburse the agency for Medicaid services rendered
- County billing by AHCA Finance and Accounting for hospital and nursing facility payments

c) Medical Review, Utilization Review, Pre-certification and Pre-authorization of Services

The Agency may use and disclose PHI for medical review, utilization review, pre-certification and pre-authorization of functions. Examples are:

- Prior authorization by the Medicaid workforce and contracted health care consultants to determine if certain services are medically necessary and appropriate
- Service authorization by Medicaid field office staff to determine if certain services for children are medically necessary and appropriate
- Recipient assessment for Assisted Living for the Elderly and the Aged and Disabled Waiver services by the Florida Department of Elder Affairs' contractors

- Comprehensive Assessment and Review for Long Term Care Services (CARES) preadmission screening for nursing facility and certain home and community-based service waiver services
- Preadmission and Annual Screenings and Annual Resident Reviews (PASARR) on nursing facility recipients who suffer from mental illness or are developmentally delayed as required by federal regulations
- Children's Multidisciplinary Assessment Team (CMAT) assessment to determine the medical necessity of certain services for children with special needs. Medicaid field office staff participates in these reviews
- Utilization review by a private contractor to safeguard against unnecessary and inappropriate medical care
- Developmental Disabilities assessments to determine medical necessity for ICF/DD services and the Developmental Disabilities and Supported Living Waivers
- Certification of home health services in excess of the service limits by the CMAT for children or pre-certification contractor for adults and children
- Sub-acute Inpatient Psychiatric Program (SIPP) assessment by the behavioral health care utilization management contractor
- Specialized Therapeutic Foster Care staffing for certification of services
- Authorization of inpatient psychiatric and substance abuse services by the pre-certification contractor
- Authorization to receive certain organ transplant services by the AHCA Organ Transplant Advisory Council
- Authorization of certain transportation services by the Medicaid field offices or transportation coordinators
- Prior authorization by the Therapeutic Consultation Program contractor to authorize certain pharmaceuticals

Health Care Operations

Agency operations activities include, but are not limited to:

a) Quality assessment and improvement activities
b) Reviewing the competency and qualifications of providers
c) Training workforce members
d) Contract renewal and cost setting
e) Legal services
f) Audit functions
g) Fraud and abuse detection
h) Compliance programs
i) Business planning and development
j) Management activities
k) Distributing information to recipients

Examples of these activities are listed below:

a) Quality Assessment and Improvement Activities
The Agency may use or disclose PHI for quality assessment and improvement activities.

Examples are:

- Quality assessment and improvement activities performed by the Medicaid Division and its contractors, the Florida Center for Health Information and Policy Analysis and its contractors, and the Health Quality Assurance Division, including outcome evaluation and development of clinical guidelines and protocols.
- Disease management by contracted vendors who provide information about treatment alternatives to recipients and providers.

b) Reviewing the Competence and Qualifications of Health Care Providers

The Agency may use and disclose PHI for provider credentialing and enrollment activities. Examples are:

- Medicaid credentialing community mental health and certain home and community-based waiver providers
- Medicaid Provider Enrollment approving certain provider types for enrollment
- Medicaid field office site surveys and quality of care reviews for credentialing, re-credentialing and continuing participation of primary care providers

c) Training Workforce Members

The Agency may use PHI for the purpose of training its workforce as necessary and appropriate for the worker's job duties.

d) Contract Renewal and Cost-Setting

The Agency may use and disclose PHI for contract renewal and cost-setting activities.
Examples are:

- Medicaid Program Analysis rate setting for facilities and clinic encounters
- Division of Medicaid and Division of Health Quality Assurance approving, monitoring, and renewing HMO contracts

e) Legal Services, Auditing Functions, Fraud and Abuse Detection, and Compliance Programs

The Agency may use and disclose PHI for legal services, auditing functions, and fraud and abuse detection and compliance programs.
Examples are:

- Provision of legal services by the General Counsel
- Provider audits by Medicaid workforce members and its contractors
- Fraud and abuse detection and activities by Medicaid Program Integrity and the Medicaid Fraud Control Unit

f) Business Planning and Development

The Agency may use and disclose PHI for business planning and development activities. Examples are:

- Cost-management and planning-related analyses related to managing and operating Medicaid by the Division of Medicaid
- Development of quality improvement initiatives by the contracted Peer Review Organization designed to improve quality and/or reduce the cost of care

- Development of policies on covered services, guidelines, and protocols by the Division of Medicaid
- Review and approval of drug use criteria and standards for both prospective and retrospective drug use by the Drug Utilization Review Panel
- Evaluation of practitioner prescribing patterns, development of educational interventions to promote the proper use of medications, and recommendation of ways to incorporate the interventions in practitioners' practices by the Prescribing Pattern Review Panel
- Review of a preferred drug list by the Medicaid Pharmaceutical and Therapeutics Committee

g) Management Activities

The Agency may use and disclose PHI for management activities. Examples are:

- Customer service functions for applicants, recipients, and providers by all Medicaid bureaus, field offices, and Agency executive staff
- Complaint and problem resolution by Health Quality Assurance field operations and field offices
- Complaint and problem resolution by the Agency executive staff, i.e., the Agency Secretary, the Communications Office and the Inspector General's Office
- Resolution of internal worker grievances by the Agency
- De-identification of data by the Division of Medicaid that is used for research, analysis, cost setting, coverage, and limitations
- Review of Child Health Check-Up reports and referring recipients for Child Health Check-Up services by the Medicaid field offices
- Case management and care coordination by the Medicaid field offices

h) Distribution of Information to Medicaid Applicants and Recipients

The Agency may use and disclose PHI to distribute the following types of information to applicants and recipients:

- Communications directly related to the administration of the Medicaid program. This includes information about what types of services are covered, co-payments and coinsurance amounts, and participating providers
- Communications made to recipients as part of the management of the recipient's care. This includes communication about products, services, therapies or other types of treatments, including those offered by third parties, as part of the management of the recipient's health. This includes disease management correspondence and Women and Infant Care (WIC) referrals
- Appointment reminders such as the Child Health Check-Up letters
- Materials directly related to the health and welfare of applicants and recipients, such as announcements of free medical exams, availability of surplus food, and consumer protection information
- Complaint resolution letters
- Voter information and registration materials as required by the National Voter Registration Act

3. The Minimum Necessary Standard

45 CFR 164.502(b)
45 CFR 164.514(d)
HITECH Act §13405(b)

When using or disclosing PHI, the Agency must make reasonable efforts to limit the use or disclosure to the minimum necessary to accomplish the intended purpose of the use or disclosure.

For example, send only the specific record requested, not the whole file.

The Minimum Necessary Standard does not apply to:

a) Disclosures to a health care provider for treatment
b) Uses or disclosures made to the individual who is the subject of the PHI
c) Uses or disclosures made pursuant to a valid authorization
d) Disclosures made to the Secretary of HHS in the course of an investigation or compliance review
e) Disclosures that are required by law

4. Verification

45 CFR 164.514(h)

Prior to any disclosure of PHI, Agency workers must:

a) Verify the identity of a person requesting PHI, and the authority of the person to have access to the PHI (if the identity of the person is not known to the worker); and
b) Obtain any documentation, statements, or representations (whether oral or written) from the person requesting the PHI, when required as a condition of the disclosure

Procedure

Workers must follow the verification procedures outlined below. *See Chapter One, Section B-1, below.*

Requests from legislators about a constituent's PHI must be forwarded to the Legislative Affairs Office and to the HIPAA Privacy Officer. *See Chapter One, Section C-5.*

Requests from public officials (law enforcement, etc.) concerning PHI should be forwarded to the HIPAA Privacy Officer.

If a worker is uncertain whether a person has the authority to request PHI, or whether the person's identity is adequately verified, the worker should consult with the work unit supervisor or the HIPAA Privacy Officer.

B. When an Authorization is Not Required

The following section describes the types of uses and disclosures of PHI that do not require a worker to obtain an authorization from the individual who is the subject of the PHI.

1. Disclosures to the Individual

45 CFR 164.502(a) and (b)
45 CFR 164.524
45 CFR 164.528

The Agency is permitted to disclose PHI to the individual who is the subject of the information (upon verification of the identity of the individual).

The Minimum Necessary Standard (above) does not apply to disclosures made to the individual. *See Chapter One, Section A-3.*

Procedure

Before disclosing any PHI to an individual, all workers shall make a reasonable, diligent effort to verify that the individual requesting the information is in fact the individual who is the subject of the information. Use the following identity verification procedures at a minimum, to verify the identity of the requester:

a) For in-person inquiries, the individual must provide a government-issued photo identification card with a photograph that closely resembles the individual; or
b) For telephone inquiries, all workers should verify identity by requesting proof that the individual knows at least two identifiers. *For example: Social Security number and Medicaid number.* The worker should verify the accuracy of the identifiers by using the information in the Agency's files or databases

For each disclosure of PHI, the Agency worker shall document that verification was obtained, and the means of verification.

If a worker discovers that a requester submitted false identification, the worker should immediately notify the work unit supervisor and the HIPAA Privacy Officer.

Note that there is a distinction between disclosing PHI to individuals in the form of answering a questions, and formal requests by individuals to obtain a copy of PHI, or to inspect PHI. If individuals requests copies of records containing PHI, to inspect records containing PHI, or an accounting of disclosures of health information, the requests must be submitted to the HIPAA Privacy Officer. *See Chapter Three, Sections D & F.*

2. Disclosures to Personal Representatives, Parents, Guardians and Executors

45 CFR 164.502(g)
45CFR 164.510(b)(5)

The Agency must treat a personal representative as if that person is the individual who is the subject of the information for the purpose of determining whether to disclose PHI. A personal representative is a person who under law has the authority to act on behalf of an individual in making decisions related to health care, e.g., someone who is a designated health care surrogate.

Parents and Guardians

The Agency must treat a custodial parent, guardian, or other person who has the legal authority to act on behalf of an unemancipated minor as a personal representative when determining whether to disclose the PHI.

A person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual to request PHI if:

a) Permitted by law; or
b) A custodial parent, guardian, or other person with legal authority consented to an agreement of confidentiality between a health care provider and the minor with respect to the health care service.

However:

a) If prohibited by state or other law, the Agency may not disclose PHI about an unemancipated minor to a parent, guardian or other person acting with legal authority; and
b) When the parent, guardian, or other person acting with legal authority is not the minor's personal representative under the above requirements, and where there is no applicable access provision under state or other law, the Agency may provide or deny access if such action is consistent with state or other applicable law, provided that such a decision is made by a licensed health care professional.

Abuse, Neglect or Endangerment Situations

The Agency may elect not to treat a person as the personal representative of an individual if the Agency has a reasonable belief that:

a) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
b) Treating such person as the personal representative could endanger the individual, and the Agency, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as a personal representative

Deceased Individuals

The HIPAA privacy rights of deceased individuals continue for 50 years beyond the date of death. The Agency must treat an executor, administrator, or other person who has authority to act on behalf of a deceased individual or an estate, as a personal representative when determining whether to disclose PHI. The PHI must be relevant to the personal representation. The Agency may disclose PHI of a deceased individual to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Agency.

Procedure

Agency workers shall verify the identity and authority of the person requesting PHI on behalf of another individual. For each disclosure, the worker shall document that verification was made, and the means of verification.

If an Agency worker receives a request from a person requesting PHI on behalf of an individual, and has a reasonable belief that the individual may have been or may be subjected to domestic violence, abuse, or neglect by the person, the Agency worker shall exercise professional judgment in determining whether to disclose the PHI, and whenever possible, advise and consult with the work unit supervisor and the HIPAA Privacy Officer to assist in determining whether to make the disclosure. If a denial of a request is made to a personal representative on this basis, the denial must be documented, and promptly reported to the HIPAA Privacy Officer. The documentation must be maintained for six (6) years.

3. Other Uses and Disclosures about Decedents

45 CFR 164.512(g) and (h)

Coroners and Medical Examiners

The Agency may disclose PHI of a decedent to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

Funeral Directors

The Agency may disclose PHI of a decedent to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. The Agency may also disclose the PHI prior to, and in reasonable anticipation of, the individual’s death, if necessary for funeral directors to carry out their duties.

Cadaveric Organ, Eye, or Tissue Donation

The Agency may disclose PHI of a decedent to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the

purpose of facilitating organ eye or tissue donation and transplantation.

Procedure

These requests should be forwarded to the HIPAA Privacy Officer.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

4. Disclosures to Business Associates and Other Government Agencies

45 CFR 164.502(e)
HITECH Act §§13401 and 13404

The Agency may disclose PHI to an Agency business associate, or to a government agency, and may allow it to create or receive PHI on its behalf, if the Agency obtains satisfactory assurance that the business associate or government agency will appropriately safeguard the information. *See Chapter Two, Section J. See also the definition of "Business Associate" in Appendix "A" – Glossary.*

Note: this standard does not apply to disclosures made by the Agency to health care providers concerning the treatment of an individual.

Procedure

For each business associate or government agency with whom the Agency shares PHI, the Agency shall ensure that there is a Business Associate Agreement (BAA) or Interagency Agreement in place between the Agency and the entity, in which the entity agrees to the rules that safeguard the privacy of PHI. The Agency maintains a standard BAA executed with all contracts involving PHI.

Workers shall verify that there is a contract in place with the business associate or government agency before disclosing any PHI to it. Ask your supervisor or the HIPAA Privacy Officer if you are uncertain whether there is a contract and BAA in place. This requirement applies to all Agency procurement types, including purchase orders, where PHI held by the Agency is disclosed to the vendor.

If any worker receives information or otherwise becomes aware that a business associate or government agency is failing to adequately safeguard PHI that is provided to the entity by the Agency, the worker should notify the work unit supervisor and the HIPAA Privacy Officer.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

5. Uses and Disclosures Required by Law

45 CFR 164.512(a)

The Agency may use or disclose PHI to the extent that such use or disclosure is required by law.

Procedure

When disclosing PHI required by law, workers must follow the requirements specific to the situation. See the subsections on Disclosures About Victims of Abuse, Neglect or Domestic Violence; Disclosures for Law Enforcement Purposes; and Disclosures for Judicial and Administrative Proceedings. All requests for disclosure of PHI for these purposes must be referred to the HIPAA Privacy Officer unless the worker has a good-faith belief that emergency circumstances exist and life, health, or safety is at risk. In such a case, the worker making the disclosure must notify the HIPAA Privacy Officer as soon as possible following the disclosure.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

6. Uses and Disclosures for Public Health Activities

45 CFR 164.512(b)

The Agency is permitted to use PHI for its public health activities. The Agency may use or disclose PHI for public health activities to:

a) Another public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to the reporting of disease, injury, vital events such as birth or death, and the conduct of public surveillance, public health investigations, and public health interventions; or to an official of a foreign government agency that is acting in collaboration with a public health authority;
b) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
c) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-related product or activity, for which that person has responsibility for activities related to the quality, safety or effectiveness of the product or activity (refer to 45 CFR 164.512(b)(iii) for further information); or
d) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the Agency is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

Procedure

Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

7. Disclosures to Government Entities Providing Public Benefits

45 CFR 164.512(k)(6)

The Agency may disclose PHI relating to eligibility for or enrollment in a health plan to another agency administering a government program providing public benefits, if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

The Agency may also disclose PHI relating to a government program to another agency administering a program providing public benefits serving the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of the programs.

Procedure

Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

8. Use and Disclosure for Health Oversight Activities

45 CFR 164.512(d)

The Agency may request and/or use PHI for its health oversight activities.

The Agency may disclose PHI to another health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

a) The health care system;
b) Government benefit programs for which health information is relevant to recipient eligibility;
c) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
d) Entities subject to civil rights laws for which health information is necessary for determining compliance.

Exception to Health Oversight Activities

A health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity, and the investigation or other activity does not arise out of and is not directly related to:

a) The receipt of health care;
b) A claim for public benefits related to health; or
c) Qualification for or receipt of public benefits or services when a patient's health is integral to the claim for public benefits or services.

Procedure

Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

9. Disclosures Regarding Victims of Abuse, Neglect or Domestic Violence

45 CFR 164.512(c)

The Agency may disclose PHI about an individual whom the Agency reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

a) To the extent the disclosure is required by law, and the disclosure complies with the requirements of the law;
b) If the individual agrees to the disclosure; or
c) To the extent the disclosure is expressly authorized by statute or regulation, and the Agency, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims (if the individual is unable to agree because of incapacity, the Agency may disclose PHI to a law enforcement or other public official authorized to receive the report, if the official represents that the PHI sought is not intended to

be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure).

Informing the Individual

If the Agency makes a disclosure regarding victims of abuse, neglect, or domestic violence, the Agency must promptly inform the individual that such a report has been or will be made, except if:

a) The Agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
b) The Agency would be informing a personal representative, and the Agency reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interest of the individual, as determined by the Agency in the exercise of professional judgment.

Procedure

If you receive a request for PHI from a social service or protective services agency relating to abuse, neglect, or domestic violence, check with the HIPAA Privacy Officer before disclosing any PHI.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

10. Disclosures to Law Enforcement

45 CFR 164.512(f)

The Agency may disclose PHI for a law enforcement purpose to a law enforcement officer if the conditions below are met:

Pursuant to Process and as Otherwise Required by Law

The Agency may disclose PHI as required by law, including laws that require the reporting of certain types of wounds or other physical injuries or in compliance with:

a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
b) A grand jury subpoena; or
c) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that (a) the information sought is relevant and material to a legitimate law enforcement inquiry; (b) the request is specific and limited in scope to the extent reasonably practicable in light of the

purpose for which the information is sought; and (c) de-identified information could not reasonably be used.

Limited Information for Identification and Location Purposes

The Agency may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that the Agency may disclose only the following information:

a) Name and address
b) Date and place of birth
c) Social Security number
d) ABO blood type and Rh factor
e) Type of injury
f) Date and time of treatment
g) Date and time of death, if applicable
h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos

Victims of a Crime

The Agency may disclose PHI in response to a law enforcement official's request for information about an individual who is, or is suspected to be a victim of a crime, if:

a) The individual agrees to the disclosure; or
b) The Agency is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that (a) the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (b) the law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (c) the disclosure is in the best interests of the individual as determined by the Agency, in the exercise of professional judgment.

Decedents

The Agency may disclose PHI about an individual who has died to law enforcement officials for the purpose of alerting law enforcement of the death of the individual, if the Agency has a suspicion that such death may have resulted from criminal conduct.

Crime on Premises

The Agency may disclose to a law enforcement official PHI that the Agency believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the Agency.

Procedure

If you receive a request for PHI from law enforcement, contact the HIPAA Privacy Officer for approval before disclosing the PHI. In an emergency situation, exercise good professional judgment as detailed above when deciding whether to disclose information to law enforcement. Be sure to verify the identity and authority of the law enforcement official, and then notify your supervisor and the HIPAA Privacy Officer as soon as possible about the disclosure.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

11. Uses and Disclosures to Avert a Serious Threat to Health or Safety

45 CFR 164.512(j)

The Agency may, consistent with applicable law standards of ethical conduct, use or disclose PHI, if the Agency, in good faith, believes the use or disclosure:

a) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
b) Is necessary for law enforcement authorities to identify or apprehend an individual, because of a statement by an individual admitting participation in a violent crime, which the Agency reasonably believes may have caused serious physical harm to the victim, or where it appears that the individual has escaped from a correctional institution or from lawful custody.

Limited Disclosure

Under item b) above conditions, the Agency may disclose to law enforcement only the statement made by an individual admitting participation in a violent crime, and the following information:

a) Name and address
b) Date and place of birth
c) Social security number
d) ABO blood type and Rh factor
e) Type of injury
f) Date and time of treatment
g) Date and time of death, if applicable
h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos

Procedure

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the

Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

12. Uses and Disclosures for Specialized Government Functions

45 CFR 164.512(k)

National Security and Intelligence Activities

The Agency may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

Protective Services for the President and Others

The Agency may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state, or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Correctional Institutions and Other Law Enforcement Custodial Situations

The Agency may disclose to a correctional institution or a law enforcement official having custody of an inmate or other individual, PHI about the inmate or individual, if the correctional institution or official represents that the information is necessary for:

a) The provision of health care to such individuals
b) The health and safety of such individual or other inmates
c) The health and safety of the officers, workers or others at the correctional institution, or persons responsible for transporting of inmates between facilities, institutions, or settings
d) The administration and maintenance of the safety, security, and good order of the correctional institution

Procedure

If you receive a request from a national security official, federal official, law enforcement, or a correctional institution for PHI, refer the request to the HIPAA Privacy Officer.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

13. Disclosures for Judicial and Administrative Proceedings

45 CFR 164.512(e)

The Agency may disclose PHI in the course of any judicial or administrative proceeding:

a) In response to an order of a court or administrative tribunal, provided that the Agency discloses only the PHI expressly authorized by such order; or
b) In response to a subpoena, discovery request, or other lawful process, if the Agency receives satisfactory assurances from the party seeking the PHI (see below).

Satisfactory Assurance

The Agency may disclose PHI in compliance with a subpoena, discovery request or other lawful process, if the party seeking the PHI provides satisfactory assurance in the form of a written statement and accompanying documentation demonstrating that:

a) The party has made a good faith attempt to provide written notice to the individual; the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and time to raise an objection has elapsed and either no objections were filed, or all objections have been resolved by the court or tribunal and the disclosures being sought are consistent with the resolution; or
b) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the party seeking the request has requested a qualified protective order from the court or tribunal.

Qualified Protective Order

A qualified protective order means an order of a court or of an administrative tribunal, or a stipulation by the parties to the litigation or administrative proceeding that:

a) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
b) Requires the return of the PHI or its destruction, including all copies made, at the end of the litigation or proceeding.

Procedure

Prior to disclosing any information in response to a subpoena, discovery request, or other lawful process, workers shall obtain satisfactory assurances as detailed above and shall contact the HIPAA Privacy Officer for approval prior to disclosing the PHI. The HIPAA Privacy Officer shall coordinate with the Office of General Counsel as necessary.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

14. Disclosures for Worker's Compensation

45 CFR 164.512(l)

The Agency may disclose PHI as authorized by laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

15. Disclosures to the Secretary of HHS

45 CFR 164.502(a)(2)

The Agency is required to disclose PHI when requested by the Secretary of HHS to investigate or determine the Agency's compliance with the HIPAA Privacy and Security Rule.

Procedure

All workers shall cooperate with the agents of the Secretary of HHS. If a worker is contacted by an agent of the Secretary of HHS, the worker should notify the work unit supervisor and the HIPAA Privacy Officer.

16. Office Sign-In Sheets

Agency offices that have visitor sign-in sheets for security purposes may require individuals who visit the office to sign in. However, the sign-in sheet may not include any other information that would make the sign-in sheets PHI, such as the purpose of the visit (if health-related or related to payment for health care services). Offices that receive visits from Medicaid recipients may not request that the recipient include an address on the sign-in sheet.

C. When an Authorization Is Required

45 CFR 164.508(a)

Except where otherwise permitted or required by the HIPAA Security and Privacy Rule, the Agency may not use or disclose written PHI without a valid, written HIPAA authorization form. The Agency's use and disclosure of that information must be consistent with the authorization.

1. Valid Authorizations

45 CFR 164.508(b) and (c)

A valid authorization must be written in plain language, and include:

a) A description of the PHI to be used or disclosed in a specific and meaningful fashion;
b) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
c) The name or other specific identification of the person(s), or class of persons, to whom the Agency may make the requested use or disclosure;
d) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
e) An expiration date or an expiration event that relates to the individual or the purpose of the disclosure. The statement, "end of the research study," "none," or similar language is sufficient if the authorization is for the use or disclosure of PHI for research;
f) The signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be provided;
g) A statement of the individual's right to revoke the authorization in writing, and the exceptions to the right to revoke, and a description of how the individual may revoke the authorization;
h) A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization; and
i) A statement of the potential for the information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by the HIPAA Security and Privacy Rule.

Defective Authorizations

An authorization is <u>not</u> valid if the document submitted has any of the following defects:

a) The expiration date has passed or the expiration is known by the Agency to have occurred;
b) The authorization has not been filled out completely with respect to any material elements;
c) The authorization is known by the Agency to have been revoked;
d) The authorization is a compound authorization or a conditional authorization (except as set forth below); or
e) Any of the material information in the authorization is known by the Agency to be false.

Compound Authorizations

An authorization for use or disclosure of PHI may not be combined with any other document, except:

a) An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same research study, except when the Agency has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations; and
b) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

Prohibition on Conditioning of Authorizations

The Agency may not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization by an individual, except under certain circumstances permitted by law.

Revocation of Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the Agency has taken action in reliance upon the authorization (a revocation cannot be retroactive).

Copy of Authorization

If the Agency seeks an authorization from an individual for a use or disclosure of PHI, the Agency must provide the individual with a copy of the signed authorization.

Documentation

The Agency must document and retain any signed authorizations for no less than six (6) years.

Procedure

If the individual is a Medicaid recipient, the Agency's Medicaid HIPAA authorization form must be used. These forms are available on the Agency HIPAA Office internet site. The Agency can accept a written authorization that is not submitted on the Agency's authorization form, provided that the authorization complies with the above requirements of law. Any exception to the use of Agency forms must be approved by the Agency HIPAA Privacy Officer prior to the disclosure of any written PHI.

Agency workers shall not use or disclose PHI unless the use or disclosure is either (1) authorized by law, or (2) authorized by the individual in the written format and containing the information required above. All completed authorization forms shall be submitted to the HIPAA Privacy Officer for approval prior to disclosing PHI.

2. Disclosures Requiring Authorization: Psychotherapy Notes

45 CFR 164.508(a)(2)

As applicable, the Agency must obtain an authorization for any use or disclosure of psychotherapy notes, except for:

a) Use by the originator of the psychotherapy notes for treatment;
b) Use or disclosure by the Agency to defend itself in a legal action or other proceeding brought by the individual;

c) Use or disclosure by the Secretary of HHS in the course of an investigation or compliance review of the Agency;
d) Use or disclosure required by law; or
e) Use or disclosure to a health oversight agency for oversight activities.

Procedure

Workers shall obtain an authorization from the individual for any use or disclosure of psychotherapy notes for reasons other than listed above. If a worker is uncertain whether a particular use or disclosure of psychotherapy notes is permitted under a certain situation, the worker should consult with the work unit supervisor or the HIPAA Privacy Officer prior to use or disclosure.

3. Disclosures Requiring Authorization: Research

45 CFR 164.512(i)

The HIPAA regulations define "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

The Agency may use or disclose PHI for research, regardless of the source of funding of the research, provided that:

a) An Institutional Review Board (IRB) established in accordance with federal law, or Privacy Board established to review research proposals has waived the requirement that the Agency obtain the authorization from the individual who is the subject of the PHI;
b) The Agency obtains assurances from the researcher that the PHI will be reviewed for purposes preparatory to research; or
c) The Agency obtains assurances from the researcher that the use or disclosure sought is solely for research on the PHI of decedents.

Researcher's Assurances that Review of PHI is Preparatory to Research

The Agency must obtain assurances from the entity conducting the research that:

a) The use or disclosure of the PHI is sought solely to review the information as necessary to prepare a research protocol or for similar purposes preparatory to research;
b) No PHI is to be removed from the Agency facilities by the researcher in the course of the review; and
c) The PHI for which use or access is sought is necessary for the research purposes.

Researcher's Assurances that Research is on Decedent's Information

The Agency must obtain from the entity conducting the research:

a) Assurances that the use or disclosure of the PHI is sought solely for research on decedents;
b) Documentation of the death of such individuals; and
c) Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

Criteria for Waiver of Authorization for Research

The IRB or Privacy Board must determine that the use or disclosure of the PHI for the research involves no more than minimal risk to an individual's privacy based on:

a) An adequate plan to protect the identifiers from improper use and disclosure;
b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
c) Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted.

The IRB or Privacy Board must also make a determination that the research could not practicably be conducted without access to the PHI.

Waiver Approval

The research must be approved in writing by the IRB or Privacy Board and contain the following documentation:

a) A statement identifying the IRB or Privacy Board and the date on which the waiver of authorization was approved;
b) A statement that the IRB or Privacy Board has determined that the waiver of authorization meets the above listed criteria;
c) A brief description of the PHI for which use or access was determined to be necessary;
d) A statement that the research has been approved under either normal or expedited review procedures; and
e) Signature of IRB's or Privacy Board's chair or other member, as designated by the chair, on the waiver of authorization.

Institutional Review Board

An Institutional Review Board must follow the requirements of the Common Rule, including the normal review procedures provided in federal law (see the Code of Federal Regulations).

Privacy Board Membership

The Privacy Board must meet the following membership requirements:

a) It must have members with varying backgrounds and appropriate professional competency as

necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

b) It must include at least one member who is not affiliated with the Agency, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
c) It must not have any member participating in a review of any project in which the member has a conflict of interest.

Privacy Board Procedures

The Privacy Board must meet the following requirements to approve research:

a) Review the proposed research at convened meetings;
b) A majority of the Privacy Board members must be present, including at least one member who is not affiliated with the Agency, any entity conducting or sponsoring the research, and not related to any person affiliated with any of these entities; and
c) The research must be approved by the majority of the Privacy Board members, unless the Privacy Board elects to use the expedited review procedure.

Privacy Board Expedited Review Procedure

A Privacy Board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI. If the Privacy Board elects to use an expedited review procedure, the review and approval of the research may be carried out by the chair, or by one or more members designated by the chair.

Procedure

Whenever possible, workers should use de-identified data or a limited data set for research purposes. *See Chapter One, Sections E-1 and E-2*. De-identified information or information in a limited data set does not have to comply with the requirements of this section. If de-identified information or a limited data set is not an option, then either written authorization must be obtained from the individual or a waiver must be sought from an IRB or the Agency Privacy Board.

Note that most of the research activities performed by the Division of Medicaid are for Medicaid operational purposes, and are not considered "research" by HIPAA's definition.

Any worker that wishes to use PHI for a research project, or receives a request from a business associate or outside entity that wishes to use PHI in the possession of the Agency to conduct a research project, must obtain approval from the HIPAA Privacy Officer before using or disclosing PHI for the research project.

The HIPAA Privacy Officer will make a determination whether the research project proposal needs to be submitted to an IRB or the Agency Privacy Board for approval. The HIPAA Privacy Officer shall appoint the members of the Privacy Board.

4. Disclosures Requiring Authorization: Marketing and Sale of PHI

45 CFR 164.508(a)(3) and (4)

A covered entity must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

a) A face-to-face communication made by the covered entity to an individual; or
b) A promotional gift of nominal value provided by the covered entity.

If the marketing involves direct or indirect payment to the covered entity from a third party, whose product or service is being described, the authorization must state that such remuneration is involved.

An authorization must be obtained for the sale of PHI and the authorization must state that the disclosure will result in remuneration to the Agency.

Procedure

In general, these provisions are not applicable to the Agency, as the Agency does not engage in marketing or sale of PHI. However, if a worker wishes to engage in a marketing activity, the worker must first obtain approval from the HIPAA Privacy Officer. The HIPAA Privacy Officer must also approve any Agency disclosure of PHI that results in any form of remuneration or that might in any way be considered a sale of PHI.

Medicaid: Agency workers may not use information about Medicaid recipients for marketing purposes, nor may PHI of Medicaid recipients be sold.

5. Disclosures Requiring Authorization: Legislators Inquiring About Constituents' PHI

Any worker who receives a request for information from a legislator or a legislator's staff must contact the Agency's Legislative Affairs Office.

If the legislator or the legislator's staff only wants confirmation after the review and completion of the constituent inquiry that the situation was resolved, no authorization is needed because no PHI was released to the legislator. If the legislator or the legislator's staff requires detailed information that includes PHI, then the worker should politely inform the legislator of the HIPAA requirement that we cannot release protected health information to anyone other than the individual who is the subject of the information without a signed authorization from the individual. The worker shall offer to provide the legislator with the authorization form. The HIPAA Privacy Officer shall review the completed form for approval of PHI release.

The original, signed authorization shall be maintained for six (6) years. Workers who receive requests from legislators should forward a copy of the authorization to Legislative Affairs and to the HIPAA Privacy Officer.

6. Uses and Disclosures Requiring Authorization: All Other Uses and Disclosures

For any other use or disclosure of PHI that is not expressly authorized by law, Agency workers must obtain a written authorization from the individual who is the subject of the PHI and approval of the HIPAA Privacy Officer prior to disclosing the PHI.

If you have any questions regarding whether you are authorized to use or disclose PHI, you should contact your supervisor or the HIPAA Privacy Officer before using or disclosing the PHI.

D. When an Individual Must Be Given an Opportunity to Agree or Object

Under the circumstances described below, the Agency may use or disclose PHI, provided that the individual is informed in advance, and has the opportunity to agree, to prohibit, or restrict the use or disclosure. The Agency may orally inform the individual, and may obtain the individual's oral agreement.

1. Use and Disclosure for Involvement in the Individual's Care

45 CFR 164.510

The Agency may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

With the Individual Present

If the individual is present for, or otherwise available prior to, a use and disclosure permitted above, and has the capacity to make health care decisions, the Agency may use or disclose the PHI if it:

a) Obtains the individual's agreement;
b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
c) Reasonably infers from the circumstances, based upon the exercise of professional judgment that the individual does not object to the disclosures.

When the Individual Is Not Present

If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Agency may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual, and if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. The Agency may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

2. Use and Disclosure for Notification or When the Individual is Deceased

45 CFR 164.510

The Agency may use or disclose PHI to notify, or assist in the notification of (including identifying or locating) a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, of the individual's location, general condition, or death. If the individual is deceased, the Agency may disclose to the aforementioned individuals who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Agency.

Procedure

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

3. Use and Disclosure for Disaster Relief Purposes

45 CFR 164.510

The Agency may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The requirements of allowing the individual the opportunity to agree or object to such use and disclosure apply to the extent that the Agency, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Procedure

Medicaid: Despite this provision of HIPAA, the Agency may not disclose information about Medicaid recipients unless the disclosure is directly connected with the administration of the Medicaid State Plan. Check with your supervisor or with the HIPAA Privacy Officer prior to disclosing information if you are uncertain whether the disclosure is appropriate.

E. De-Identification and Limited Data Sets

One way to protect the privacy of an individual is to strip the health information of its identifying data before using or disclosing the health information. This section provides the procedures for two methods of stripping PHI of identifiers: De-Identification and Limited Data Sets.

1. De-Identification

45 CFR 164.502(d)

45 CFR 164.514(a) & (b)

De-identified information, essentially, is health information that has been stripped of all of its identifying data. The resulting de-identified health information is no longer subject to the restrictions on PHI and may be used and disclosed.

The Agency may determine that health information is not individually identifiable health information only if: (1) the identifiers are removed and the Agency does not have knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information (known as the "HIPAA Safe Harbor De-identification Method"); or (2) a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying such principles and methods, determines that the risk is very small that the information could be used to identify the subject of the information and documents the methods and results of the analysis that justify such determination (known as the "HIPAA Expert Determination De-identification Method").

Identifiers

Please see Chapter One, Section A-1 for a list of identifiers.

Re-Identification

The Agency may assign a code or other means of record identification to allow de-identified information to be re-identified by the Agency, provided that:

a) The re-identification code is not derived from or related to information about the individual, and is not otherwise capable of being translated so as to identify the individual; and
b) The Agency does not use or disclose the re-identification code for any other purpose.

Procedure

All data and documents published or publically disclosed must be de-identified. The Agency's preferred method of de-identifying PHI is the HIPAA Safe Harbor De-identification Method whereby all identifiers are stripped from the data or documents prior to disclosure. Agency approved redaction software shall be used for electronic redaction. Employees shall utilize the HIPAA Safe Harbor De-identification Method to de-identify PHI or shall contact the HIPAA Privacy Officer for approval to utilize the HIPAA Expert Determination De-identification Method. The releasing worker's supervisor is responsible for ensuring information is properly redacted/de-identified prior to disclosure.

2. Limited Data Sets

45 CFR 164.514(e)

Essentially, a limited data set is PHI that has been stripped of most (but not all) of its identifiers.

The Agency may use or disclose a limited data set only for the purposes of research, public health, or health care operations of the Agency. Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

The Agency may disclose a limited data set only if the Agency enters into a Data Use Agreement with the person or organization that requests the information.

The following identifiers of the individual who is the subject of the PHI, or the individual's relatives, employers or household members must be removed:

a) Names
b) Postal address information, other than town or city, state, and zip code
c) Telephone numbers
d) Fax numbers
e) Electronic mail addresses
f) Social Security numbers
g) Medical record numbers
h) Health plan recipient numbers
i) Account numbers
j) Certificate/license numbers
k) Vehicle identifiers and serial numbers, including license plate numbers
l) Device identifiers and serial numbers
m) Web Universal Resource Locators (URLs)
n) Internal Protocol (IP) address numbers
o) Biometric identifiers, including fingerprints, and voiceprints
p) Full face photographic images and any comparable images

Data Use Agreement

A data use agreement between the Agency and the limited data set recipient must at a minimum:

a) Establish the permitted uses and disclosures of the information by the limited data set recipient. The agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of the Privacy Rule if done by the Agency;
b) Establish who is permitted to use or receive the limited data set; and
c) Provide that the limited data set recipient will:
    1. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    3. Report to the Agency any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
    4. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient

with respect to such information; and
5. Not re-identify or contact the individual(s).

Compliance

The Agency is in violation of the Privacy Rule, if the Agency knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the Agency took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

a) Discontinued disclosure of PHI to the recipient; and
b) Reported the problem to the Secretary of HHS.

Procedure

Workers must follow applicable Agency policies and procedures for limited data set development and review routing prior to data disclosure. If a worker is uncertain about the proper creation, use, or disclosure of a limited data set, the worker should consult with the work unit supervisor or with the HIPAA Privacy Officer before using or disclosing any PHI. Any worker that becomes aware that a recipient of a limited data set is misusing the data in violation of the Privacy Rule or of the data use agreement, should report the violation immediately to the work unit supervisor and to the HIPAA Privacy Officer.

F. Improper Use and Disclosure

Violating the Privacy Rule can have serious repercussions in the form of employment sanctions, civil penalties, or even criminal fines and imprisonment.

1. Duty to Mitigate Harm

45 CFR 164.530(f)
HITECH Act §§13401 and 13404

The Agency must mitigate, to the extent practicable, any harmful effect that is known to the Agency of a use or disclosure of PHI in violation of its policies and procedures or the requirements of the Privacy Rule by the Agency or its business associate.

Procedure

Any Agency worker, who discovers that the Agency or a business associate has violated the Privacy Rule or the Agency's procedures, must immediately report the violation to the HIPAA Privacy Officer who will coordinate the Agency's mitigation efforts.

2. Employee Sanctions

45 CFR 164.530(e)

The Agency must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Agency or the requirements of the Privacy Rule.

This provision does not apply to workers who disclose PHI as whistleblowers, or as crime victims reporting to a law enforcement official, in accordance with 45 CFR 164.502(j). *See Chapter One, Section F-5*.

Refraining from Intimidating or Retaliatory Acts

No Agency worker shall intimidate, threaten, coerce, discriminate against, or retaliate against any member of the public who files a complaint with the Agency regarding an alleged privacy violation, or who requests access to their PHI. Any Agency employee who engages in intimidating, coercive, discriminatory, or retaliatory acts against a member of the public for filing a complaint or requesting access shall be subject to employment sanctions. *See Chapter 4, Section B.*

Documentation

The Agency must document the sanctions that are applied, if any.

Procedure

Department of Management Services Rule 60L-36.005(e), "Disciplinary Standards" provides that an employee may be disciplined for "violation of law or agency rules." Employees shall abide by the law and applicable rules and policies and procedures, including those of the employing agency and the rules of the State Personnel System. All employees are subject to Part III of Chapter 112, Florida Statutes, that govern standards of conduct, which agencies shall make available to employees. An agency may determine that an employee has violated the law, even if the violation has not resulted in arrest or conviction. Employees shall abide by both criminal law, for example, drug laws, and civil law, for example, laws prohibiting sexual harassment and employment discrimination.

Any employee who violates the Agency's policies and procedures, or state or federal laws governing privacy may be subject to discipline, up to, and including termination of employment. The HIPAA Privacy Officer shall be responsible for documenting any sanctions that are applied. The documentation shall be maintained for six (6) years.

3. Penalties Under the Law

42 USC 1320d-5
HITECH Act §13409
45 CFR 160.400-424

General Penalties under HIPAA and HITECH

Section 13409 of the HITECH Act clarifies that criminal penalties established by HIPAA may apply to an individual or worker of the Agency who obtains, uses or discloses PHI without proper authorization.

If the Secretary of HHS or the HHS Office for Civil Rights determines that a person has failed to comply with a provision of HIPAA, under the HITECH Act, the Secretary of HHS shall impose a penalty of not more than $50,000 for each violation. The total amount of penalties imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

A penalty may not be imposed if it is established to the Secretary of HHS' satisfaction that the person liable did not know, and by exercising reasonable diligence would not have known, that the person violated the provision.

A penalty may not be imposed if the failure to comply was due to reasonable cause and not due to willful neglect; and the failure to comply is corrected during the thirty (30) day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. This period may be extended by the Secretary of HHS based upon the nature and extent of the failure to comply. If the Secretary of HHS determines that the person failed to comply because the person was unable to comply, the Secretary of HHS may provide technical assistance to the person.

The HITECH Act authorizes the State Attorney General to file lawsuits on behalf of state residents whose PHI has been used or disclosed in an unauthorized manner.

Unauthorized or Wrongful Disclosure of PHI under HIPAA

42 USC 1320d-6
HITECH Act §§13410 and 13411
45 CFR 160.402-408

A person who knowingly, and in violation of HIPAA uses or causes to be used a unique health identifier, obtains individually identifiable health information relating to an individual, or discloses individually identifiable health information to another person, shall:

a) Be fined not more than $50,000, imprisoned not more than 1 year, or both;
b) If the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years or both; and
c) If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

4. Breach Notification Requirements

45 CFR 164.402-412

HITECH Act §§13401, 13402 and 13404

Both the Agency and its business associates have a legal duty to notify certain parties in the event of a breach of "unsecured PHI." The definition of "unsecured PHI" means PHI that has not been either encrypted or destroyed thereby rendering the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

The term *breach* means the unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

The term *breach* does not include:

a) Any unintentional acquisition, access, or use of protected health information by a worker or individual acting under the authority of a covered entity or business associate if:
    1. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such worker or individual, respectively, with the covered entity or business associate; and
    2. Such information is not further acquired, accessed, used, or disclosed by any person; or
b) Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and
c) Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Procedure

Workers shall notify the Agency HIPAA Privacy Officer immediately but not later than one business day from discovery of all unauthorized disclosures made by the Agency. The HIPAA Privacy Officer or delegate shall coordinate breach investigation, response activities, and shall conduct a breach risk assessment documenting the probability of PHI compromise based on the following four factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

An unauthorized disclosure is presumed to be a breach unless the breach risk assessment process concludes that there is a low probability of PHI compromise. In the event of a breach, the Agency

will provide written notice via first-class mail to the affected persons or next-of-kin, as applicable under the HIPAA rule, within sixty (60) days of discovery date. If there is insufficient contact information for fewer than ten (10) affected individuals then substitute notice will be provided by other available means, such as telephone contact. If there is insufficient contact information for ten (10) or more affected individuals that precludes a written notice, a conspicuous posting on the Agency's web site for a period of ninety (90) days, or notice in major print or broadcast media that includes a toll-free number that will remain active for at least ninety (90) days, will occur. If unsecured information of more than 500 people is involved, notice must be made to local media. Notice must also be provided to the Secretary of HHS contemporaneously with the individual notifications for breaches affecting 500 or more. Such notice must be made in the manner specified on the HHS website. If less than 500 people are involved in a breach, the Agency will submit the breach report not later than sixty (60) days after the end of each calendar year to the Secretary in the manner specified on the HHS website.

Individual breach notification may be delayed if a law enforcement official states to a covered entity or business associate that a breach notification notice, or posting required would impede a criminal investigation or cause damage to national security, per 45 CFR 164.412.

Notification to individuals and the media, as applicable, must include:

a) A brief description of events surrounding the breach;
b) Types of information involved;
c) Steps individuals should take to protect themselves from harm;
d) Steps the Agency is taking to investigate and mitigate harm; and
e) Contact procedures for those seeking more information.

Additionally, any breach of Medicaid recipient data, whether committed by an Agency workforce member, business associate, or subcontractor, must be reported to the Agency Medicaid Fiscal Agent Operations (MFAO) to determine the need to contact Social Security Administration (SSA). MFAO will make this determination and any subsequent notification.

A business associate must follow the terms of its Business Associate Agreement with the Agency, which includes notifying the Agency of the details of the breach, when it happened, and who was impacted.

5. Disclosures by Whistleblowers and Workforce Member Crime Victims

45 CFR 164.502(j)

Whistleblowers

The Agency is not considered to have violated the Privacy Rule if a member of its workforce or a business associate discloses PHI, provided that:

a) The workforce member or business associate believes in good faith that the Agency has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or

that the care, services, or conditions provided by the Agency potentially endangers one or more patients, workers, or the public; and

b) The disclosure is to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Agency, or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Agency; or an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining legal options with regard to the whistleblowing conduct.

Workforce Members Who Are Victims of Crime

The Agency is not considered to have violated the Privacy Rule if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that:

a) The PHI disclosed is about the suspected perpetrator of the crime; and
b) The PHI disclosed is limited to the information permitted to disclosures to law enforcement for identification and location purposes. *See Chapter One, Section B-10.*

Procedure

Workers who wish to disclose PHI under the above conditions should carefully comply with the limitations of the law, take reasonable means to safeguard the PHI, and disclose the minimum necessary PHI to accomplish the objective. Whenever possible, the worker should also notify the HIPAA Privacy Officer.

Chapter Two:
Safeguards

42 CFR 431.300-307
45 CFR 164.308-312
45 CFR 164.530(c)

HIPAA requires the Agency to develop appropriate and reasonable safeguards to protect the privacy of PHI. Medicaid regulations also require the Agency to safeguard information regarding Medicaid applicants and recipients. The following are some basic, minimum safeguards to follow in your work unit.

Your work unit may use more stringent safeguards, but they must, at minimum include the safeguards listed below.

Remember, you may be held personally accountable if you mishandle PHI.

For example: if you take PHI home, and a family member or friend acquires it, you may be subject to the penalties listed in Chapter One, Section F-3, as well as subjecting yourself and the Agency to a possible lawsuit.

A. General Requirements

The Agency must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

Agency workers must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements of the Privacy and Security Rule.

Agency workers must also reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Procedure

If you have any questions about the safeguards in your work unit, please contact your supervisor or the HIPAA Privacy Officer.

B. Vocal, Telephone and Voice Mail Safeguards

Workers should not talk about an individual's PHI in public areas within the workplace, such as elevators, reception areas, the cafeteria, or outside of the workplace where an unauthorized worker or visitor could overhear the conversation.

Do not play back voice mail messages on speakerphone if the message might contain PHI.

Your voice mail should be password-protected. Do not give out your voice mail password to any non-Agency employee, and do not post or keep your password written down where it can be readily found by someone else (especially do not tape it to your desk or the side of your computer).

C. Mail Safeguards

Make sure that incoming open mail that contains PHI is not left sitting in a shared workspace, including staff mailboxes. Incoming mail should be delivered directly or picked up from the mailroom by the assigned person(s) in each work unit and kept secure until it can be distributed.

Outgoing mail that contains PHI should leave your office in a sealed envelope. If this is not possible due to specific circumstances, you must take reasonable precautions to safeguard the privacy of the PHI. Ensure mailing address on the package/envelope matches the intended address and individual.

If mailing documents containing PHI from an off-site work location, employees must deliver the sealed envelope/package to a secure collection depository or with an employee of a courier service. Documents are not to be left on a mail counter or for home pick-up.

D. Fax Safeguards

When you fax PHI, make sure that it is sent with a cover sheet that includes a confidentiality statement, and call the recipient immediately before and after sending the fax to ensure that it is expected and picked up promptly.

For incoming faxes, fax machines should be located in an area where the assigned person(s) can ensure that faxes are kept confidential and are promptly distributed to the proper recipient. Fax machines should not be located in areas such as reception areas where visitors can view incoming faxes. Faxes containing PHI awaiting pickup should not be posted or pinned to bulletin boards in common areas.

E. Email Safeguards

When you forward or copy an email to someone outside of the Agency, first make sure that it does not contain PHI anywhere in the email chain or attachments unless the individual receiving the email is authorized to access the PHI. Do not create rules in your Agency email account to auto forward any emails to a non-Agency account.

Access to your email is password-protected through the network login screen. Do not share your password with anyone. Do not leave a copy of your password on a piece of paper where it can be easily found (especially do not tape it to your desk or the side of your computer screen).

Use of personal email accounts and other non-Agency email accounts by workers to create, access, receive, maintain, or transmit PHI or other confidential and/or exempt information is prohibited.

For further guidance, refer to *Agency IT and HR policies* on acceptable email use.

Email Encryption

All emails that contain PHI or any other confidential information sent to non-Agency email addresses must be encrypted. To encrypt an email, simply type the word ENCRYPT at the beginning or end of the subject line; this will encrypt the email and make it apparent to the recipient of the email that it contains PHI/confidential information. Those emails are easy to locate in your Sent folder when you search for them later. A best practice is to put ENCRYPT in the subject line of **all** emails containing PHI, whether or not they are sent outside the Agency network (i.e., to non-Agency email addresses). **Do not put PHI or other confidential information in the subject line of the email since the subject line itself is not encrypted.**

For detailed instructions on how to send and open encrypted emails, contact the IT Help Desk.

Emails containing PHI need to be retained under the same requirements as other documentation under HIPAA (retained for at least six (6) years, if part of the Designated Record Set – *See Chapter Three, Section D. See also the definition of "Designated Record Set" in Appendix "A" – Glossary*).

F. Computer Safeguards

All *Agency Information Technology Policies and Procedures* are incorporated by reference into this policy and procedure manual and are available on the Agency's Policies and Procedures website.

Use of non-Agency approved and/or unencrypted personal devices by workers to create, access, receive, maintain, or transmit PHI or other confidential and/or exempt information is prohibited.

Do not post information, which may contain PHI or any information that could reasonably be used to identify an individual Medicaid recipient or facility patient on social media.

Save documents containing PHI onto a network server. Do not save PHI onto your hard drive. If you save PHI onto a DVD/CD, the DVD/CD must be encrypted and password protected. Only Agency-issued, encrypted USB drives are to be used with Agency computers. For further guidance on mobile devices, refer to *Agency IT Policies*. When the media is destroyed, it must be done in a HIPAA-compliant manner (for example, do not just throw a DVD/CD in the trash – it must be destroyed by shredding). For further guidance on electronic media destruction, refer to *Agency IT policies*.

Applications, databases, or network shares containing PHI should be encrypted whenever risk level indicates that encryption is appropriate as determined by the business unit in consultation with the Division of Information Technology.

Do not share your password(s) for any system containing Agency PHI (ex. network or FLMMIS) with anyone. Do not post or keep a copy of your password(s) on a piece of paper where they can be easily found (especially do not tape any passwords to your desk or the side of your computer screen).

The supervisor of each individual work unit shall be responsible for ensuring that a worker's privileges are submitted for termination no later than the effective date of termination.

Use a screen saver that activates if the computer is not in use for a maximum of 15 minutes and requires a password to log back in.

Use the "Lock" function to lock your computer whenever you leave your office.

Be aware of whether your computer screen may be easily seen by office visitors. For example, if you use PHI in your daily work, if possible you should reposition your computer screen so that it does not face the hallway or a window where unauthorized individuals might see the information on the screen.

Agency-issued Mobile Devices

Only use encrypted, Agency-issued/approved mobile devices for emailing PHI and follow the same safeguards as you would for a computer. You must safeguard the device from being accessed by anyone outside of the Agency. If your device is lost or stolen, you should promptly report the matter to your supervisor, the Information Technology Help Desk, the Information Security Manager, and to the HIPAA Privacy Officer.

Digital Copiers and Multi-Function Devices (MFDs)

Many of the Agency's leased copiers and MFDs have hard drives that retain information from copied, faxed, or printed documents. To ensure no PHI/confidential information leaves the Agency all MFD and copier internal hard drives must be wiped by the leasing vendor prior to the MFD/copier leaving the Agency office or being returned to the leasing vendor. The Agency's contracts with leasing vendors typically include this requirement. The vendor will provide written certification of the data wipe. If, however, the contract/lease agreement does not include on-premises data wiping, immediately contact the Agency's Division of Information Technology (IT) and the Division of Operations Procurement Office. Do not allow the hard drive to leave the Agency office until a data wipe has been performed and certified.

Information Technology Security Policies

In addition to the requirements under HIPAA, all workers must comply with the requirements of the Agency's Information Technology policies and procedures. A copy of the policies and procedures, including the Information Security Program Plan, is available on the Agency's Policies and Procedures internal website.

G. Office Safeguards and Physical Security Walkthroughs

All Agency Division of Operations Facilities Management and Records Management Policies and Procedures are incorporated by reference into this policy and procedure manual and are available on the Agency's Policies and Procedures website.

Do not leave papers that contain PHI open to view where non-Agency workers can see them. At the end of the workday, take all PHI off your desk or other exposed areas and secure it from open view. PHI should be reasonably secured from intentional or unintentional disclosure at all times. Follow the procedures of your individual work unit. For some work units this may mean locking the PHI in a file cabinet, for others it may mean locking the office. If you have any questions regarding your work unit's safeguards, consult with your supervisor or the HIPAA Privacy Officer.

Work unit supervisors or designated HIPAA Liaisons and HIPAA Compliance Office staff shall perform an unannounced periodic physical security walkthrough of their facilities to identify areas where PHI is not secure and assist workers in relocating information or equipment and developing procedures to prevent unauthorized access to the information. Documentation and findings of these reviews shall be sent to the HIPAA Compliance Office. The walkthrough should include:

a) Checking the location of fax machines, mail trays, and mail bins to ensure no documents containing PHI are accessible
b) Checking the location of bins for paper waiting to be shredded to ensure security and no overfilling
c) Checking the location of communal waste and recycle bins to ensure no documents containing PHI are improperly disposed of
d) Checking the maintenance and custodial procedures to ensure proper function
e) Checking record storage to ensure documents containing PHI are properly stored
f) Checking computers of unattended work spaces/offices to ensure use of the screen lock function

Found physical security issues shall be reported to the HIPAA Compliance Office and appropriate workforce member(s) and/or supervisor. Individual performing the walkthrough has the authority to address any improperly stored or disposed of document(s) and lock any unattended, unlocked computer(s). These action(s) may require entrance into an unattended work space/office. If any improperly stored documents appear to be active work documents, the documents will be immediately returned to the appropriate workforce member(s) or supervisor.

The Agency contracts with maintenance, custodial, shredding, copier service, and storage vendors shall include the Agency's standard Business Associate Agreement if PHI is to be handled or acquired (e.g., for shredding or transport off premises).

H. Safeguards for Teleworkers and Taking PHI Off-Site

Teleworkers, workers who take work off-site, must safeguard PHI from intentional or unintentional disclosure to non-Agency workers. *This includes household members and guests.* Printed PHI that is taken off-site should be kept in a locked container when being transported or

not in use, such as a locking briefcase or filing cabinet. When transporting PHI, all PHI must be secured within the locked cabin or trunk of the vehicle. Avoid carrying printed PHI outside of your office building by using Agency-issued encrypted mobile devices whenever possible. It is the sole responsibility of the worker to ensure that the PHI, whether printed or on portable media, is secure and returned to the Agency for proper disposal.

If you work from home and receive PHI on voice mail or an answering machine, you should make sure that the voice mail or answering machine is not shared with, or accessible by anyone who is not an Agency worker.

Use only Agency-issued/approved encrypted mobile computing devices or Agency solutions to conduct work requiring access to PHI. Do not use your home or personal computer without prior Agency approval. Do not save PHI to your home or personal computer or other personal device. Users must take reasonable precautions to protect printed PHI, portable media, and mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage. Printed PHI, portable media, and mobile computing devices should not be left in a vehicle. When leaving a vehicle, users should take the printed PHI, portable media, and mobile computing devices with them. If this is not possible, these items should be locked in the trunk of the vehicle. In the case of vehicles without trunks, doors should be locked with the printed PHI, portable media, and/or mobile device(s) kept out of plain sight. If a worker is working from home, the printed PHI, portable media, and/or mobile device should be placed in a secure area, such as a locking cabinet or drawer, when not in use.

If mailing documents containing PHI from an off-site work location, workers must deliver the sealed envelope/package to a secure collection depository or with an employee of a courier service. Documents are not to be left on a mail counter or for home pick-up.

If a worker has questions or concerns, they should contact the work unit supervisor, the IT Security Manager, and/or the HIPAA Privacy Officer.

I. Disposing of Printed PHI

45 CFR 164.530

Paper containing PHI that does not have to be retained must be shredded. The Agency supplies shredders and contracts with shredding vendors for on-site shredding. Printed PHI may not be left in an area where it can be viewed by an unauthorized person while waiting to be shredded. If locked shred bins are not available or are full, PHI waiting to be shredded must be stored in a locking file cabinet or a locking office until such time as an empty locked shred bin is available. Workers must be cautious not to put paper containing PHI in wastebaskets or recycle bins. If a worker is aware of PHI having been placed in regular trash, they are to retrieve the PHI and properly dispose of it by shredding or placing it in a locked shred bin. If it is not possible to retrieve the PHI (for example, it is in an inaccessible dumpster or waste receptacle), secure the trash receptacle/dumpster as much as possible by posting staff near it and telephone the HIPAA Compliance Office and your facility management representative immediately. If PHI is properly destroyed, such as by being shredded, and the destroyed PHI were to be obtained by an unauthorized party, the disclosure would not be considered to be a breach; therefore, the Agency would not be required to comply with the breach notification requirements of the HITECH Act.

Documents containing PHI that must be retained must be stored in locking file cabinets or boxes in a secure area.

J. Business Associate Contracts

45 CFR 164.504(e)
HITECH Act §§13401, 13402 and 13404

It is important to note that the HITECH Act requires business associates to comply with the Privacy Rules with regard to the handling of PHI as though they were a HIPAA covered entity.

Contract Requirements

The Agency's standard Business Associate Agreement (BAA) is an attachment to all Agency contracts where the vendor creates, receives, maintains, or transmits PHI on behalf of the Agency. The BAA establishes the permitted uses and disclosures of PHI by the business associate. The BAA prohibits the business associate from using or disclosing the information in a manner that would violate the Privacy Rule and it authorizes termination of the contract by the Agency if the Agency determines that the business associate has violated a material term of the contract.

The BAA also provides that the business associate will:

a) Not further use or disclose the information other than as permitted or required by the contract or as required by law;
b) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
c) Report to the Agency any use or disclosure of the information not provided for by its contract

of which it becomes aware;

d) Ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by the business associate on behalf of, the Agency agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
e) Make PHI available in accordance with the Right of Access. *See Chapter 3 Section D*;
f) Make PHI available for amendment and incorporate any amendments to PHI in accordance with the Right to Amend. *See Chapter 3 Section E*;
g) Make available the information required to provide an accounting of disclosures in accordance with the Right to an Accounting of Disclosures. *See Chapter 3 Section F;*
h) Make its internal practices, books, and records of PHI received from, or created or received by the business associate on behalf of the Agency available to the Secretary of HHS for the purpose of determining the Agency's compliance with the Privacy Rule; and
i) At the termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the Agency that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information, and limit further uses and disclosures to those purposes that make the return or the destruction of the information infeasible.

Noncompliance by a Business Associate

The Agency has violated the Privacy Rule if the Agency knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement unless the Agency has taken reasonable steps to cure the breach or end the violation and, if unsuccessful, has either:

a) Terminated the contract or arrangement, if feasible; or
b) If termination is not feasible, reported the problem to the Secretary of HHS.

Procedure

For each business associate with whom the Agency shares PHI, the Agency shall ensure that the Agency's current standard Business Associate Agreement (BAA) is in place between the Agency and the business associate in which the associate agrees to comply with the requirements of the Privacy and Security Rule. The BAA shall provide that the business associate must receive written approval from the Agency before the business associate may share the information with any other entity.

All workers shall verify that there is a contract with a BAA in place with the business associate before disclosing any PHI to the business associate. Ask your supervisor, the Agency Procurement Office or the HIPAA Privacy Officer if you are uncertain whether there is a contract and current BAA in place.

If any worker receives information or otherwise becomes aware that a business associate is failing to adequately safeguard PHI, the worker should notify the work unit supervisor and the HIPAA Privacy Officer.

K. Interagency Agreements

45 CFR 164.504(e)(3)

If the business associate is a governmental agency, the Agency may enter into a Memorandum of Understanding (MOU) with the other agency in lieu of entering into a formal Business Associate Agreement (BAA) as specified above. The memorandum must contain terms that accomplish the same objectives as those required in a BAA.

The Agency may also dispense with entering into a BAA with another government agency if other law or regulations contain requirements that accomplish the same objectives as those required in a BAA.

The Agency may omit from its arrangements the requirement that it terminate the contract with the government agency if such termination is inconsistent with the statutory obligations of the Agency or its business associate.

Procedure

Generally, the Agency will enter into an "Interagency Agreement" (or "Data Sharing Agreement" or "Data Use Agreement" or "Memorandum of Understanding") with other governmental agencies, which contains the same terms as those used in Business Associate Agreement (see previous section).

If any worker receives information or otherwise becomes aware that a government agency is failing to adequately safeguard PHI that is provided by AHCA, the worker should notify the work unit supervisor and the HIPAA Privacy Officer.

Chapter Three:
Rights of Individuals

HIPAA establishes greater rights to individuals to have access to their PHI.

Among other rights, members of the public have: (1) the right to be notified of the Agency's privacy practices; (2) the right to access their PHI; (3) the right to amend their PHI; (4) the right to request an accounting of who the Agency has disclosed their PHI to other than for purposes of treatment, payment, health care operations, disclosures to the patient, national security purposes or disclosures to law enforcement; (5) the right to restrict how the Agency uses and discloses their PHI; and (6) the right to request communications of PHI by alternative means if it will otherwise endanger them.

A. Notice of Privacy Practices

45 CFR 164.520

An individual has a right to adequate notice of:

a) Certain uses and disclosures of PHI that may be made by the Agency;
b) The individual's rights under the Privacy Rule; and
c) The Agency's legal duties with respect to PHI.

The Agency must provide a notice that is written in plain language, containing specific content as provided in 45 CFR 164.520(b).

The Agency must promptly revise and distribute its notice whenever there is a material change in the uses or disclosures, the individual's rights, the Agency's legal duties, or other privacy practices stated in the notice. Except where required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

The Agency must provide notice of its privacy practices to Medicaid recipients at the time of enrollment. If there is a material revision to the notice, the Agency must provide the revised notice within sixty (60) days of the revision. Once every three years, the Agency must notify Medicaid recipients of the availability of the notice or how to obtain the notice. Individuals have the right to obtain a paper copy of the notice upon request.

Procedure

The Agency is required to have a Notice of Privacy Practices. The Notice of Privacy Practices is to be provided to new Medicaid recipients at the time of enrollment and no less frequently than once every three years or if there is a material change to the notice the Agency must notify Medicaid recipients of the availability of the notice and how to obtain it. The Agency's Notice of Privacy Practices is posted on the Agency's public web site. The HIPAA Privacy Officer shall be

responsible for implementing any revisions to the notice. Requests for a paper copy of the notice may be referred to the HIPAA Privacy Officer.

B. Right to Request Restrictions of Uses and Disclosures

45 CFR 164.522(a)

The Agency must permit an individual to request that the Agency restrict uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations and disclosures permitted under 45 CFR 164.510(b).

The Agency is not required to agree to a restriction. If the Agency agrees to a restriction, the Agency may not use or disclose PHI in violation of the restriction except if the individual is in need of emergency treatment and the PHI is needed to provide the emergency treatment. If the information is given to a health care provider for emergency treatment, the Agency must request that the health care provider not further use or disclose the information.

The Agency may not agree to restrict uses and disclosures: (1) to the Secretary of HHS to investigate or determine the Agency's compliance with the Privacy Rule; (2) for a facility directory pursuant to 45 CFR 164.510; or (3) any use or disclosure under 45 CFR 164.512 (e.g., uses and disclosures required by law, for public health activities, victims of abuse, neglect or domestic violence, for health oversight activities, for judicial or administrative proceedings, for certain law enforcement purposes, for decedents, for research purposes, to avert a serious threat to health or safety, for specialized government functions, or for workers' compensation).

The Agency may terminate its agreement to a restriction if the individual agrees to or requests the termination in writing, the individual orally agrees to the termination and the oral agreement is documented, or the Agency informs the individual that it is terminating its agreement to a restriction (the termination is only effective with respect to the PHI created or received after the Agency has informed the individual).

Procedure

A request for a restriction must be submitted in writing to the HIPAA Privacy Officer, using the Agency restriction form. The HIPAA Privacy Officer shall make a determination whether to accept or deny the request. Before a request may be accepted, the request must be reviewed by the Division Director(s) of the affected bureau(s), or designee(s). The HIPAA Privacy Officer shall be responsible for communicating the acceptance or the denial to the individual who made the request and, if accepted, shall communicate the restriction to the affected bureaus and document the restriction.

C. Right to Request Confidential Communications by Alternative Means or at Alternative Locations

45 CFR 164.522(b)

The Agency must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the Agency by alternative means or at alternative locations if the individual clearly states that the disclosure of all or part of that information by regularly established means could endanger the individual.

Procedure

Requests to receive communications by alternative means must be submitted through a completed Agency HIPAA request form to the HIPAA Privacy Officer and: (1) must clearly state that the disclosure of all or part of the information could endanger the individual, and (2) must specify an alternative address or other method of contact. The HIPAA Privacy Officer will evaluate the validity and reasonableness of the request, respond to the individual, and, if accepted, will communicate the request to the affected bureau. If the change must be made by another agency, a staff member may refer the individual to the appropriate agency (e.g., address changes to FLMMIS for Medicaid recipients must be made by the Department of Children and Families).

D. Right of Access to PHI

45 CFR 164.524

An individual has the right to inspect and obtain a copy of PHI about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

Providing Access

The Agency must provide the individual with access to the PHI in the form or format requested by the individual, including electronically if requested by the individual, and if it is readily producible in such form or format or, if not, in a readable hard copy form or such other form or format as agreed to by the Agency and individual.

The Agency may provide the individual with a summary of the PHI requested in lieu of providing access or may provide an explanation of the PHI if the individual agrees in advance to receiving a summary or explanation and to the fees imposed, if any.

The Agency must provide access in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI or mailing the copy of the information at the individual's request. The Agency may discuss the scope, format, and other aspects of the request for access with the individual to facilitate the timely provision of access.

Fees

The Agency may impose a fee for copying or for providing the information in an alternative format.

Denial of Access

The Agency may deny an individual access without providing an opportunity for review in the following circumstances:

a) The records requested are psychotherapy notes;
b) The information was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
c) The records are subject to the Privacy Act of 1974, 5 U.S.C. 552a; or
d) The PHI was obtained from someone other than a health care provider under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information.

The Agency may deny an individual access, provided that the individual is given a right to have such denials reviewed, in the following circumstances:

a) A licensed health care professional has determined, in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
b) The PHI makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
c) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

Review of Denial by Licensed Health Care Professional

If access is denied because of one of the grounds listed above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Agency to act as a reviewing official and who did not participate in the original decision to deny access. The designated reviewing official must determine within a reasonable period of time whether or not to deny the access requested. The Agency must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required to carry out the official's determination.

Partial Denial

If the Agency denies access in part to PHI, the Agency must give the individual access to any other PHI requested after excluding the PHI as to which access was denied.

Form of Denial

The denial must be written in plain language, and contain the basis for the denial, a statement of the individual's review rights (if applicable) and a description of how the individual may complain to the Agency or to the Secretary of HHS.

If the Agency does not maintain the PHI that is the subject of the individual's request for access, and the Agency knows where the requested information is maintained, the Agency must inform the individual where to direct the request for access, if known.

Timely Action

Within thirty (30) days of receipt of a request for access to PHI that is maintained or accessible by the Agency on-site, the Agency must either inform the individual of the acceptance of the request or provide a written denial.

If the Agency is unable to take action within the time limitations above, the Agency may extend the time by no more than thirty (30) days, provided that the Agency provides a written statement of the reasons for the delay and the date by which the Agency will complete its action on the request. The Agency may have only one extension of time.

Documentation

The Agency must document and retain for no less than six (6) years the designated record sets that are subject to access by individuals and also document the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Procedure

All requests for access to written PHI must be immediately submitted to the HIPAA Privacy Officer. The HIPAA Privacy Officer shall review the requests and make a determination as to whether to allow or deny access and shall communicate with the individual making the request in the manner and within the time limitations required by law. The HIPAA Privacy Officer shall designate a licensed health care professional to review requests for access, as needed, as well as a second licensed health care professional to evaluate requests for review of denial of access. All workers shall cooperate with and assist the HIPAA Privacy Officer in copying or providing access to inspect PHI.

If a worker receives a phone or in-person request for access to a Medicaid recipient's PHI, the worker may refer the person to the HIPAA Privacy Officer or, alternatively, may assist the person in preparing a request for PHI using either the Agency's HIPAA access or authorization form available on the Agency's HIPAA Compliance Office internet website. The worker may inform the individual of options with regard to access (copying, summary or inspection). The form must then be immediately submitted by the worker to the HIPAA Privacy Officer either electronically or by fax. The worker shall verify the identity of the person requesting the PHI. Requests from personal representatives for access must be sent in writing, signed by the personal representative, to the HIPAA Privacy Officer. The written request must document proof of the personal representative's legal authority to access the requested information.

The Agency may assess a fee for copying pursuant to the requirements of Section 119.07, Florida Statutes.

The HIPAA Privacy Officer shall be responsible for maintaining documentation of the designated record set for no less than six (6) years.

E. Right to Amend PHI

45 CFR 164.526

An individual has the right to have the Agency amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

Timely Action

The Agency must grant an amendment or provide a written denial to an individual within sixty (60) days after receipt of the request. The Agency may extend the time by no more than thirty (30) days if the Agency is unable to act within the time required. The Agency must provide the individual with a written statement of the reasons for the delay and the date by which the Agency will complete its action on the request. The Agency may have only one such extension per request.

Making the Amendment

If the Agency accepts the requested amendment, in whole or in part, the Agency must make the amendment to the PHI by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

The Agency must inform the individual in a timely manner that the amendment is accepted and obtain the individual's identification of and agreement to have the Agency notify the relevant persons with which the amendment needs to be shared. The Agency must make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as having received the PHI and needing the amendment and persons (including business associates) that the Agency knows have the PHI that may have relied, or foreseeably could rely, on such information to the detriment of the individual.

Denial of Request for Amendment

The Agency may deny an individual's request for amendment if it determines that the PHI or record that is the subject of the request:

a) Was not created by the Agency, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
b) Is not part of the designated record set;
c) Would not be available for inspection under the Right of Access provisions; or
d) Is accurate and complete.

The Agency must provide the individual with a timely denial, written in plain language, containing: (1) the basis for the denial; (2) the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement (the Agency can

reasonably limit the length); (3) a statement that if the individual does not submit a statement of disagreement, the individual may request that the Agency provide the request for amendment and the denial with any future disclosures of the PHI; and (4) a description of how the individual may file a complaint with the Agency or with the Secretary of HHS. The Agency may prepare a written rebuttal to the statement of disagreement, which must be provided to the individual.

Recordkeeping

The Agency must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Agency's denial of the request, the individual's statement of disagreement, if any, and the Agency's rebuttal, if any, to the designated record set.

Actions on Notices of Amendment

If the Agency is informed by another covered entity of an amendment to an individual's PHI, the Agency must amend the PHI in its designated record sets.

Documentation

The Agency must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation for no less than six (6) years.

Procedure

All requests for amendment must be submitted in writing to the HIPAA Privacy Officer who will determine whether to accept the amendment and shall communicate the acceptance or denial to the individual. The HIPAA Privacy Officer may prepare written rebuttals to statements of disagreement on behalf of the Agency as needed.

All Notices of Amendment from other covered entities shall be forwarded to the HIPAA Privacy Officer, who shall be responsible for coordinating the documentation of the amendment with the applicable Agency Bureau.

If the change must be made by another agency, a staff member may refer the individual to the appropriate agency (for example, address changes to FLMMIS for Medicaid recipients must be made by DCF).

F. Right to an Accounting of Disclosures

45 CFR 164.528
HITECH Act §13405(c)

An individual has a right to receive an accounting of disclosures of PHI made by the Agency in the six (6) years prior to the date on which the accounting is requested. Please note that the

individual can request an accounting of a period of time of less than six (6) years.

Denial of Request for an Accounting of Disclosures

The Agency is not required to account for disclosures made:

a) To carry out treatment, payment or health care operations;
b) To individuals about their PHI;
c) Incident to a use or disclosure otherwise permitted by the Privacy Rule;
d) Pursuant to an authorization;
e) For a facility's directory or to persons involved in the individual's care, or other notification purposes as provided in 45 CFR 164.510;
f) For national security or intelligence purposes;
g) To correctional institutions or law enforcement officials; or
h) As part of a limited data set.

Temporary Suspension of Accounting Upon Request by Law Enforcement

The Agency must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight or law enforcement official, if the agency or official provides the Agency with a written statement that such an accounting to an individual would be reasonably likely to impede the agency's or official's activities, and must specify the time for which such a suspension is required. If the agency or official makes an oral statement, then the Agency can limit the temporary suspension to no longer than thirty (30) days. The Agency must document the statement, including the identity of the agency or official making the statement.

Content of the Accounting

For each disclosure, the accounting must include:
a) The date of the disclosure;
b) The name of the entity or person who received the PHI and, if known, the address of such entity or person;
c) A brief description of the PHI disclosed; and
d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of the disclosure or, in lieu of such a statement, a copy of a written request for disclosure, if any.

Accounting of Multiple Disclosures to the Same Entity for the Same Purpose

If, during the period covered by the accounting, the Agency has made multiple disclosures to the same person or entity for a single purpose, the Agency may provide (in addition to the above) the date of the first accounting; the frequency, periodicity, or number of the disclosures made during the accounting period; and the date of the last such disclosure during the accounting period (so as to avoid having to list each and every single disclosure separately).

Accounting of Disclosures for Research

If the disclosure was made for a particular research purpose for fifty (50) or more individuals, the accounting may provide: (1) the name or the protocol or other research activity; (2) a brief description, in plain language, of the activity, including the purpose of the research and the criteria for selecting particular records; (3) a brief description of the type of PHI that was disclosed and the date or period of time during which the disclosures occurred; (4) the name, address, and telephone number of the entity that sponsored the research and of the research to whom the information was disclosed; and (5) a statement that the PHI may or may not have been disclosed for a particular protocol or other research activity. If it is reasonably likely that the PHI was disclosed for a research activity, the Agency shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Timely Action

The Agency must provide an accounting to an individual no later than sixty (60) days after receiving the request. The Agency may extend the time by an additional thirty (30) days if unable to provide the accounting within the specified time. The Agency must provide the individual with a written statement of the reasons for the delay and the date by which the Agency will provide the accounting. The Agency may have only one such extension of time.

Cost of the Accounting

The Agency must provide the first accounting to an individual in any twelve (12) month period without charge. The Agency may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the twelve (12) month period. The Agency must inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Documentation

The Agency must document and retain for six (6) years the information required to be included in an accounting for disclosures of PHI; the written accounting provided to the individual; and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Procedure

Requests for an accounting of disclosures of PHI must be submitted on the Agency form to the HIPAA Privacy Officer, who will evaluate the request, coordinate the gathering of information from the Agency, prepare the accounting, and communicate with the individual. All workers shall cooperate with and assist the HIPAA Privacy Officer in researching and preparing the accounting. The Bureaus shall be responsible for maintaining the documentation of the disclosures of PHI. The HIPAA Privacy Officer shall be responsible for maintaining the documentation of the written accountings provided to individuals.

Chapter Four:
Complaint Process, Investigations, and Administrative Requirements

Members of the public also have the right to file a complaint either with the Agency or with the Secretary of HHS. This section also details additional administrative requirements under HIPAA.

A. Complaint Process

45 CFR 164.530(d)

The Agency must provide a process for individuals to make complaints concerning the Agency's policies, its failure to comply with its policies and procedures, or the requirements of the Privacy Rule.

Documentation

The Agency must document all complaints received and their disposition, if any, and maintain this documentation for six (6) years.

Procedure

All complaints must be submitted in writing to the HIPAA Privacy Officer at the following address:

HIPAA Privacy Officer
Agency for Health Care Administration
2727 Mahan Drive, Mail Stop #4
Tallahassee, Florida 32308
850-412-3960

The HIPAA Privacy Officer shall review complaints and refer to the Inspector General as necessary. The HIPAA Privacy Officer is responsible for documenting all complaints and their dispositions, if any.

B. Refraining from Intimidating or Retaliatory Acts

45 CFR 164.530(g)

The Agency may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against any individual for the exercise of any right under the Privacy Rule, including:

a) The filing of a complaint;
b) Testifying, assisting, participating in an investigation, compliance review, or hearing; or

c) Opposing any act or practice in violation of the Privacy Rule (provided the person has a good faith belief that the practice is unlawful, the opposition is reasonable, and does not involve a disclosure of PHI).

C. Compliance Reviews and Investigations by HHS

45 CFR 160.310

The Agency must keep records and submit compliance reports necessary for the Secretary of HHS to ascertain whether the Agency is complying with the Privacy Rule.

The Agency must cooperate with the Secretary of HHS (or the Secretary's designee), if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the Agency to determine whether it is complying with the Privacy Rule.

The Agency must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, that are pertinent to ascertaining compliance with the applicable requirements of the Privacy Rule. If an exigent circumstance exists, such as when documents may be hidden or destroyed, the Agency must permit access by the Secretary at any time and without notice.

Procedure

The HIPAA Privacy Officer shall be the point of contact for any investigation or compliance review by the Secretary of HHS. The HIPAA Privacy Officer shall be responsible for preparing and submitting compliance reports to the Secretary of HHS. All Agency workers shall cooperate with requests from the Secretary of the HHS in the course of an investigation or compliance review.

D. Personnel Designations: HIPAA Privacy Officer

45 CFR 164.530(a)

The Agency must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the Agency.

The Agency must designate a contact person or office responsible for receiving complaints under this section and able to provide further information about matters covered by the Notice of Privacy Practices.

Procedure

The Agency has created the position of HIPAA Privacy Officer who shall be responsible for fulfilling the above requirements of law and other related duties. The HIPAA Privacy Officer reports to the Inspector General.

E. Policies and Procedures

45 CFR 164.530(i)

As a covered entity, the Agency and work units within the Agency must develop policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the Privacy Rule. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to PHI undertaken by the Agency to ensure such compliance.

Changes to Policies and Procedures

The Agency must change its policies and procedures as necessary and appropriate to comply with the changes in the law, including the standards, requirements, and implementation specifications of the Privacy Rule.

Whenever there is a change in the law that necessitates a change to the Agency's policies or procedures, the Agency must promptly document and implement the revised policy or procedure, and, if applicable, revise and redistribute its Notice of Privacy Practices.

Procedure

The HIPAA Privacy Officer shall be responsible for updating this manual upon a change in the law or otherwise as needed.

When there is a material change in the law or the Agency's procedures, the HIPAA Privacy Officer shall ensure that all workers are trained on the new law or procedures. If the change materially affects the Notice of Privacy Practices, the HIPAA Privacy Officer shall ensure that a revised notice is distributed in accordance with the requirements of law.

F. Training

45 CFR 164.530(b)

The Agency must train all members of its workforce on the policies and procedures with respect to PHI required by the Privacy Rule as necessary and appropriate for the members of the workforce to carry out their function within the Agency.

The Agency must provide HIPAA Privacy training and Security Awareness training to each new worker within a reasonable time after the person joins the workforce and to existing workers on a periodic basis.

If the Agency makes a material change in its policies and procedures, each member of the workforce whose functions are affected by the change must be trained within a reasonable period of time after the change becomes effective.

Documentation

The Agency must document that the training described above has been provided and must maintain this documentation for six (6) years.

Procedure

The HIPAA Privacy Officer shall be responsible for developing and implementing training for the workforce on applicable privacy laws and the Agency's related procedures. Each new worker will receive training on the privacy laws and procedures as part of orientation. The HIPAA Privacy Officer and the Human Resources Bureau will maintain the training documentation.

G. Documentation

45 CFR 164.530(j)

The Agency must:

a) Maintain the policies and procedures required by the Privacy Rule in written or electronic form;
b) If a communication is required by the Privacy Rule to be in writing, maintain such writing, or an electronic copy, as documentation; and
c) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

The Agency must retain the documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Procedure

Unless otherwise specified in this manual, the HIPAA Privacy Officer shall be responsible for maintaining the documentation required by this provision.

Appendix A – Definitions

Access refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Agency means the Agency for Health Care Administration.

Agency Workforce/Worker means Agency employees, volunteers, trainees, student interns, consultants, contracted staff, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.

Business Associate is a person or entity who on behalf of the Agency:

- Performs or assists in the performance of: a function or activity involving the use or disclosure of protected information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by the HIPAA Privacy Rule; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Agency, where the provision of the service involves the disclosure of protected information from the Agency or from another Agency business associate. A covered entity may be a business associate of another covered entity. Agency workforce members are not considered to be Agency business associates.

CMS stands for the Centers for Medicare and Medicaid Services within the Department of Health and Human Services that administers Medicare and Medicaid policies. CMS used to be called the Health Care Financing Administration (HCFA). In Florida, CMS may also refer to Children's Medical Services within the Florida Department of Health.

Compliance Date is the date by which the Agency and other covered entities must comply with a standard, implementation specification, requirement, or modification adopted under the HIPAA rules. The compliance date for the HIPAA Privacy Rule is April 14, 2003.

Correctional Institution any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, Florida, a territory, a political subdivision of a Florida, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity is defined as:

- A health plan;
- A health care clearinghouse; or
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

The HIPAA regulations specifically designate Medicare, Medicaid, and the Children's Health Insurance Program as covered entities that must comply with HIPAA.

Covered Functions are those functions that a covered entity performs that make it a health plan, health care provider, or health care clearinghouse.

Data Aggregation is protected information created or received by a business associate in its capacity as an Agency business associate that the business associate combines with protected information it receives in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the Agency and the other covered entities.

Designated Record Set a group of records maintained by or for the Agency that is:

- The medical records and billing records about individuals maintained by or for a health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Agency; or
- Records used, in whole or in part, by or for the Agency to make decisions about individuals. The term record means any item, collection, or grouping of information that includes protected information and is maintained, collected, used or disseminated by or for the Agency.

Disclosure means the release, transfer, provision of access to or divulging in any other manner of information outside of the Agency.

Emancipation is when a minor has achieved independence from his or her parents, often by getting married before reaching age 18 or by becoming fully self-supporting.

Group Health Plan an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

- Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

- Is administered by an entity other than the employer that established and maintains the plan.

Note: Also, see the definition of *health plan*.

HCFA the Health Care Financing Administration within the Department of Health and Human Services that administered Medicare and Medicaid policies. HCFA is now called the Centers for Medicare and Medicaid Services (CMS).

Health Care the care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription

Health Care Clearinghouse a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

- Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or
- Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations means any of the following activities to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities including:
    - Outcomes evaluation and development of clinical guidelines provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination;
    - Contacting of health care providers and patients with information about treatment alternatives; and
    - Related functions that do not include treatment.
2. Licensing, credentialing, and training activities including:
    - Reviewing the competence or qualifications of health care professionals;
    - Evaluating practitioner and provider performance; Evaluating health plan performance;
    - Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers;
    - Training of non-health care professionals; and
    - Accreditation, certification, licensing, or credentialing activities.
3. Contract activities including:
    - Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits; and
    - Ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of Section 164.514(g) of the HIPAA regulations are met, if applicable.
4. Conducting or arranging for Medical review, Legal services, and Auditing functions.
5. Fraud and abuse detection and compliance programs.
6. Business planning and development, such as:
    - Conducting cost-management and planning-related analyses related to managing and operating the entity;
    - Formulary development and administration; and
    - Development or improvement of methods of payment or coverage policies.
7. Business management and general administrative activities of the entity, including, but not limited to:
    - Management activities relating to implementation of and compliance with the HIPAA requirements; Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected information is not disclosed to such policy holder, plan sponsor or customer;
    - Resolution of internal grievances;
    - Consistent with the applicable requirements of the HIPAA Privacy Rule, creating de-identified health information;
    - Keeping applicants and recipients informed about services, benefits, appointments, and treatment options in accordance with Federal Medicaid law and the HIPAA Privacy Rule.

Health Care Provider a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Information Health information means any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Insurance Issuer as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan, means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in Florida and is subject to state law that regulates insurance. It does not include a group health plan.

Health Maintenance Organization (HMO) As defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan, HMO means a federally qualified HMO, an organization recognized as an HMO under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as an HMO.

Health Oversight Agency Health oversight agency means an agency or authority of the United States, Florida, a political subdivision of Florida, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)). Health plan includes the following, singly or in combination:

- Group health plan;
- Health insurance issuer;
- HMO;
- Part A or Part B of the Medicare program under title XVIII of the Act;
- **The Medicaid program** under title XIX of the Act, 42 U.S.C. 1396, et seq.;
- An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1));
- An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;
- An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
- The health care program for active military personnel under title 10 of the United States Code;
- The veterans' health care program under 38 U.S.C. chapter 17;
- The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4));
- The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.;
- The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.;
- An approved state child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.;
- The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28;
- A high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals;
- Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2));

Health plan excludes:

- Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
- A government-funded program (other than the ones listed above) whose principal purpose is not providing or paying the cost of health care; or whose principal activity is the direct provision of health care to persons or the making of grants to fund the direct provision of health care to persons.

HHS is the U.S. Department of Health and Human Services.

Individual the person who is the subject of protected health information.

Individually Identifiable Health Information is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set is protected information that excludes the following direct identifiers of the applicant/recipient or of his or her relatives, employers, or household members:

1. Names;
2. Postal address information, other than town or city, state, zip code;

3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan recipient numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images

Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. Marketing excludes a communication made to an individual:

- To describe the entities participating in a health care provider network or health plan network, or to describe if, and the extent to which, a product or services (or payment for such product or service) is provided by a covered entity or included in a plan of benefits;
- For treatment of that individual; or
- For case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

Organized Health Care Arrangement is:

- A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
- An organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities that include at least one of the following:
    - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    - Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or recipients in such group health plan;
- A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
- The group health plans described above and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or recipients in any of such group health plans.

Password refers to confidential authentication information composed of a string of characters.

Payment the activities that relate to the individual to whom health care is provided undertaken by:

- A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
- A health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Payment activities include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts);
- Adjudication or subrogation of health benefit claims; and
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

Personal Representative a person who manages the legal affairs of another, such as a health care surrogate, legal guardian, power of attorney or executor.

Protected Health Information is individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in any electronic medium; or
- Transmitted or maintained in any other form or medium.

This definition excludes individually identifiable health information in:

- Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
- Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
- Employment records held by a covered entity in its role as employer.

Psychotherapy Notes are notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public Health Authority is an agency or authority of the United States, a state, a political subdivision of a state or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of the public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Record is any item, collection, or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a covered entity.

Relates to the Privacy of Individually Identifiable Health Information with respect to a state law, that the state law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Required by Law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. The HIPAA definition includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Note: In order for Medicaid protected information to be disclosed, even if required by law as defined above, the disclosure must be allowable under the Federal Medicaid regulations.

Research a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary of HHS refers to the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small Health Plan a health plan with annual receipts of $5 million or less.

Standard refers to a rule, condition, or requirement describing the following information for products, systems, services, or practices with respect to the privacy of individually identifiable health information:
- Classification of components;
- Specification of materials, performance, operations; or
- Delineation of procedures

Standard Setting Organization (SSO) an organization accredited by the American National Standards Institute (ANSI) that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State Law is a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law.

Trading Partner is an external entity, such as a third party insurer, with whom the covered entity does business. (In contrast, a business associate is an entity that performs certain business functions for a covered entity.) The same entity can be a Medicaid trading partner for some purposes and a Medicaid business associate for other purposes.

Treatment the provision, coordination, or management of health care and related services by one or more health care providers, including:
- The coordination or management of health care by a health care provider with a third party;
- Consultation between health care providers relating to a patient; or
- The referral of a patient for health care from one health care provider to another

Use with respect to individually identifiable health information means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

ACKNOWLEDGEMENT FORM

I hereby acknowledge that I have received the Agency for Health Care Administration's HIPAA/HITECH Policies and Procedures Manual.

I understand that it is my responsibility to read and follow the Agency's policies and procedures, including subsequent revisions to those policies and procedures, and all state and federal laws governing the privacy and confidentiality of information. I will request any clarification needed from the Agency's HIPAA Privacy Officer.

I understand that if I fail to follow the Agency's policies and procedures or state and federal laws governing privacy and confidentiality, I may be subject to discipline, up to and including termination of employment, as well as civil or criminal penalties.

_____ _____

Signature Date

_____

Printed Name

_____ _____

Division Bureau

This form must be turned in to the Bureau of Human Resources to be included in your personnel file.

State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER: **4031**
SUBJECT: **HIPAA/HITECH Compliance**
DIVISION: **OIG/HIPAA**
BUREAU:
SECTION:

1.0 PURPOSE/SCOPE

This policy and associated Agency HIPAA/HITECH Policies and Procedures Manual implements Agency policies and procedures required for Agency and worker compliance with the federal HIPAA/HITECH and federal Medicaid laws related to protected health information.

2.0 AUTHORITY

Health Insurance Portability and Accountability Act (1996), as amended; Health Information Technology Economic and Clinical Health Act (2009) and associated regulations (45 CFR Part 160-164); Title XI of the Social Security Act and associated regulations (42 CFR Part 431.300-307).

3.0 DEFINITIONS

Refer to the Definitions section in the Agency HIPAA/HITECH Policies and Procedures Manual.

4.0 POLICY

Refer to the Agency HIPAA/HITECH Policies and Procedures Manual, which applies to all members of the Agency's workforce to include Agency employees, volunteers, trainees, student interns, and other persons who work for the Agency in the capacity of contracted staff or consultants under the direct control of the Agency.

5.0 PROCEDURES

Refer to the Agency HIPAA/HITECH Policies and Procedures Manual.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions. Additionally, violations of HIPAA/HITECH law may result in criminal or civil penalties.

8.0 REVISION HISTORY

Author: David Herman, Privacy Officer **Date:** 2/12/2002

Approved by: N/A **Date:**

1st Revision Approved
by: David Herman, Privacy Officer **Date:** 4/14/2003

2nd Revision Approved
by: John Collins, Privacy Officer **Date:** 1/9/2008

3rd Revision Approved
by: John Collins, Privacy Officer **Date:** 11/2/2009

4th Revision Approved
by: John Collins, Privacy Officer **Date:** 7/13/2011

5th Revision Approved
by: Kathy Pilkenton, Privacy Officer **Date:** 9/20/2013

6th Revision Approved
by: Kathy Pilkenton, Privacy Officer **Date:** 5/16/2016

7th Revision Approved
by: Lisa Rodriguez, Privacy Officer **Date:** 7/24/2020

Deletion Approved
by: _____ **Date:** _____

9.0 ATTACHMENT(S)

N/A

State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER: **5009 (Previously 08-IT-06)**
SUBJECT: **Information Technology Confidential Information Policy**

DIVISION: **Information Technology**
BUREAU: **IT Strategic Planning & Security**
SECTION: **IT Security**

1.0 PURPOSE/SCOPE

To provide guidelines for the use and handling of confidential data resources.

2.0 AUTHORITY

Florida Statutes 282.318: Information Technology Security Act.

Florida Administrative Code 60GG-2: Information Technology Security.

3.0 DEFINITIONS

Availability — The principle that information and assets are accessible for those authorized.

Confidential Information — Information that is exempted from disclosure requirements under the provisions of applicable state and federal law.

Confidentiality — The principle that information is accessible only to those authorized.

Information Technology Resources — computer hardware, software, networks, devices, connections, applications, and data owned by the Agency.

Integrity — The principle that assures information remains intact, correct, and authentic.

Workforce — Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.

4.0 POLICY

To protect the confidentiality, integrity, and availability of information technology resources, Agency data must be classified as public or confidential information. The Agency will appoint information owners and approvers for Agency data. Confidential

information must be kept secured using appropriate administrative, technical, and physical safeguards. It is the responsibility of each member of the workforce to maintain security for all formats of confidential information.

5.0 PROCEDURES

Each member of the workforce is responsible for understanding whether each source of information they work with contains confidential information and applying appropriate safeguards. Safeguards must be applied in compliance with Agency policies and procedures as well as applicable state and federal rules and laws. Information Technology may review data classification and existing safeguards for confidential information.

Each member of the workforce must acknowledge these responsibilities by completing the AHCA HR Policies and Procedures Acknowledgement Form.

Agency information owners shall be responsible for classifying information as public or confidential. Agency approvers shall be responsible for authorizing access to information and maintaining documentation of users authorized to access confidential information. Confidential information shall be accessible only to authorized individuals.

Electronic transmission of confidential information must be encrypted or otherwise appropriately safeguarded when sent outside of the Agency. The agency shall implement procedures to establish accountability for accessing confidential data stores and modifying confidential data. The Agency's Information Security Manager or other authorized personnel shall be granted access to review audit logs containing accountability details. Agreements and procedures shall be in place for sharing, handling or storing confidential data with entities outside the agency.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee and each member of the workforce to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions.

Non-Agency employees and vendors are directly responsible for damage as a direct result of policy violation. Intentional and non-intentional violation can result in termination of service and may result in revocation of contract.

8.0 REVISION HISTORY

Author: Michael Scholl **Date:** 30Sept2008

Approved by: **Date:**

1st Revision Approved by: Michael Scholl & CIO **Date:** 19MAR2010

2nd Revision Approved by: Scott Ward, CIO **Date:** 10/1/2020

Deletion Approved by: _____ **Date:** _____

9.0 ATTACHMENT(S)

N/A

State of Florida
AGENCY FOR HEALTH CARE ADMINISTRATION

POLICY/PROCEDURE NUMBER:	**5013 (Previously 06-IT-04)**
SUBJECT:	**Mobile Computing Policy**
DIVISION:	**Information Technology**
BUREAU:	**IT Strategic Planning & Security**
SECTION:	**IT Security**

1.0 PURPOSE/SCOPE

To provide standards for mobile computing devices and mobile storage devices.

2.0 AUTHORITY

Florida Statutes 282.318: Information Technology Security Act.

Florida Administrative Code 60GG-2: Information Technology Security.

3.0 DEFINITIONS

Authentication – The process of verifying that a user is who he or she claims to be.

Confidential Information – Information that is exempted from disclosure requirements under the provisions of applicable state and federal law.

Encryption – Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used.

Information Technology Resources – computer hardware, software, networks, devices, connections, applications, and data owned by the Agency.

Mobile Computing Device – A laptop, smartphone, or other portable device that can process data.

Mobile Devices –both mobile computing devices and mobile storage devices.

Mobile Storage Device – Portable data storage media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW),

recordable digital videodiscs (DVD-R/RW), IPODs, media players, and cell phones or tape drives that may be easily attached to and detached from computing devices.

Firewall – a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

Remote Access – Any access to the Agency's network through a network, device, or medium that is not controlled by the Agency (such as the Internet, public phone line, wireless carriers, or other external connectivity).

Workforce — Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.

4.0 POLICY

Appropriate security controls must be in place to mitigate security risks presented by using mobile devices. All Agency security and privacy policies apply when using or connecting to Agency information technology resources from outside of an Agency facility.

The Agency's confidential information must be encrypted when transmitted over a network. Mobile devices that transmit or store the Agency's confidential information require encryption which shall include encryption when the confidential information is not in transit. To prevent loss of data, Agency data stored on mobile devices must be backed up so it does not create unique copies of Agency data.

5.0 PROCEDURES

Only mobile devices owned or managed by the Agency are allowed to directly connect to an Agency network or store Agency data. Connections shall only be through secured remote access methods approved by the Agency.

Mobile computing devices owned or managed by the Agency:

- must be tracked by the Agency,
- must use current and up-to-date anti-malware software,
- must activate a firewall that has been approved by the Agency (where technology permits) when connected to a non-Agency network,
- must install only software approved by the Agency,
- must only be issued to workforce members approved by the Agency,
- must be configured and maintained following Agency policies and procedures,
- shall require authentication unique to each member of the workforce, and
- shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.

Each member of the workforce must take reasonable precautions to protect the Agency's mobile devices in their possession from loss, theft, tampering, unauthorized access, and

damage. The Agency's Mobile computing devices should not be left in a vehicle. When leaving a vehicle, members of the workforce should take the Agency's mobile computing devices with them. If this is not possible, these devices should be locked in the trunk of the vehicle. In the case of vehicles without trunks, doors should be locked with the Agency's mobile device(s) kept out of plain sight. If an employee is working from home, the Agency's mobile device(s) should be placed in a secure area, such as a locking cabinet or drawer, when not in use.

Each member of the workforce must report theft or loss of mobile devices owned or managed by the Agency immediately to their supervisor or Agency liaison as well as the Agency's Information Security Manager.

6.0 RESPONSIBILITIES

It is the responsibility of each Agency employee and all members of the Agency workforce to comply with this policy and procedure.

7.0 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including dismissal, in accordance with Rule Chapter 60L-36, Florida Administrative Code and Agency Policy Number 96-HR-33, Disciplinary Actions.

8.0 REVISION HISTORY

Author:	**Michael Scholl**	**Date:**	1NOV2006
Approved by:	**Scott Ward**	**Date:**	12MAR2010
1st Revision Approved by:	**Michael Scholl & Scott Ward**	**Date:**	13JUL2011
2nd Revision Approved by:	Scott Ward, CIO	**Date:**	09OCT2020
Deletion Approved by:	_____	**Date:**	_____

9.0 ATTACHMENT(S)

N/A

CONTRACT MANAGER
CONFLICT OF INTEREST QUESTIONNAIRE

AHCA Contract/Agreement No.: _____

Applicable Vendor: _____

	YES	NO
1. Do you, your immediate family, or business partner have financial interest in the vendor listed above?	☐	☐
2. Do you, your immediate family, or business partner have a personal relationship with the vendor listed above or their representatives?	☐	☐
3. Have any gratuities, favors, or anything of monetary value been offered to you or accepted by you from the vendor listed above or their representatives?	☐	☐
4. Have you been employed by the above referenced vendor within the last sixty (60) months as referenced, in s.287.057(15)(a), F.S.?	☐	☐
5. Do you plan to obtain financial interest (i.e., stock) in the vendor listed above?	☐	☐
6. Have you discussed or do you plan to seek or accept future employment with the vendor listed above or their representatives?	☐	☐
7. Are there any other conditions which may cause a conflict of interest?	☐	☐

If you answered "YES" to any of the above questions, please provide a written explanation for each "YES" answer:

_____

_____

_____

_____

I DECLARE ALL OF THE ABOVE QUESTIONS ARE ANSWERED TRUTHFULLY AND TO THE BEST OF MY KNOWLEDGE.

_____ _____

Signature **Date**

_____

Printed Name

Division: Health Care Policy and Oversight
Bureau: N/A
Section: Health Care Policy

Purpose/Scope

To provide guidelines regarding the use and handling of trade secrets and confidential information pertaining to the Canadian Prescription Drug Importation Program.

Authority

Chapters 119, Florida Statutes (F.S.)

Section 688.002, F.S.

Definitions

Agency Staff – Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, whether or not they are paid by the Agency.

Canadian Prescription Drug Importation Program – As described in Section 381.02035, F.S.

Confidential Information – Information that is exempted from disclosure requirements under the provisions of applicable state and federal law.

Prescription Drug – As defined in Section 465.003, F.S.

Trade Secret – As defined in Section 688.002, F.S.

Policy

Section 119.0715, Florida Statutes (F.S.) exempts information considered to be trade secrets from disclosure in public record requests and requires state agencies to maintain confidentiality of such information. According to Section 688.002, F.S., a trade secret is defined as the following:

> *4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process that:*
>
> *(a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and*
>
> *(b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.*

The Agency considers Information obtained from manufacturers and/or distributors that is not publicly available (e.g., formulations, testing regimens) regarding products acquired for the Canadian Prescription Drug Importation Program (Program) as trade secrets that are confidential and exempt from public record. The classification of trade secret or confidential information can also apply to processes, procedures, and policies regarding the manufacturing and distribution of prescription drugs as well as the operations of the Program that fall under the definition of "trade secret" as specified in Section 688.002, F.S.

Procedures

To protect the confidentiality, integrity, and availability of prescription drug information, Agency staff will designate items deemed as trade secrets by manufacturers or companies as confidential information. Agency staff will also classify information as confidential if it falls under the definition of “trade secret” as specified in Section 688.002, F.S. Additionally, the Agency will appoint owners and approvers for such information. Confidential information must be kept secured using appropriate administrative, technical, and physical safeguards. Each Agency staff member has the responsibility to maintain security for all formats of confidential information.

To ensure each Agency staff member’s compliance with protecting confidential information, the Agency will require training in the differentiation of trade secrets and non-protected information regarding domestic and Canadian prescription drugs and how to assign classifications as appropriate.

Agency staff that will have access to trade secrets and confidential information are responsible for classifying information as public or confidential. Agency staff assigned as approvers are responsible for authorizing access to trade secrets and confidential information and maintaining documentation of authorized staff. Confidential information shall be accessible only to authorized individuals.

The Agency will require encryption or the appropriate safeguarding of electronic transmission of confidential information when sent outside of the Agency and will implement procedures to establish accountability for accessing or modifying confidential information. The Agency’s Information Security Manager or other authorized personnel will be able to review audit logs containing accountability details. The Agency will also have agreements and procedures for sharing, handling, or storing confidential information with outside entities.

Responsibilities

All Agency staff that will have access to trade secrets and confidential information regarding products, processes, and policies regarding the Program have the responsibility to comply with this policy.