Department of Health
Information Security and Privacy Policy
DOHP 50-10-16
Table of Contents

I. Policy

The Florida Department of Health (Department) possesses technology resources, data, and information that must be protected from unauthorized access, modification, destruction, and disclosure per federal and state laws.

Each Department program office, division, county health department (CHD), and Children's Medical Services (CMS) area office must have written local information security and privacy procedures to ensure the security of information and protect the confidentiality, data integrity, and access to information. Local procedures must conform to the Department Information Security and Privacy Program (ISPP) requirements as reflected in these policies and be written in approved Department format as established in DOHP 5-2, Writing, Instituting, and Revising Department Policies, IOPs, TAGs, and SOCs. Local procedures must include core security procedures required by the Department and supplemental operating procedures necessary to implement established Department policies and protocols. All procedures must be reviewed annually and updated as appropriate. Corrective action plans must be developed and implemented for all identified deficiencies.

Local entities such as CHD, CMS Area Offices, divisions, and program offices reserve the right to establish local protocols and procedures that may be more stringent. In the event of a conflict, the more restrictive measures apply.

Deviations from the Department Information Security and Privacy Policy must be requested by submitting a justification to the Information Security Manager (ISM) which includes an associated risk analysis and proposed physical, administrative and technical safeguards.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment and/or referral for criminal prosecution.

A. Information Security and Privacy Program

1. The Department of Health must maintain an agency-wide information security program to ensure administrative, operational, and technical controls are sufficient to reduce risks to the confidentiality, integrity, and availability of agency information and information technology resources.

   a) The Information Security Program must be responsive and adaptable to changing environments, vulnerabilities, and technologies affecting state information resources.

2. The State Surgeon General and the Director or Administrator of each local entity such as CHDs, CMS Area Offices, and program offices must designate key personnel with specific responsibility to coordinate the security and privacy of information for their area.

a) The State Surgeon General shall designate a Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer, a HIPAA Complaint Officer, an Information Security Manager (ISM), and a HIPAA Security Officer.

b) The Director or Administrator of each local entity shall designate at least one Information Security and Privacy Coordinator (ISPC), at least one Information Owner, at least one Information Custodian, at least one Key Custodian, at least one Disaster Recovery Coordinator, and a local HIPAA Reviewing Officer as appropriate based on Section VI.D.7. of this policy.

(1) Responsibilities must be documented in the designee(s) position description.

(2) The designee(s) identity must be documented in the local information security and privacy procedures.

(3) The identity of each ISPC must be relayed to the ISM.

II. Authority

A. Public Law (PL), 104-191, Health Insurance Portability and Accountability Act of 1996

B. 45 Code of Federal Regulations (CFR), Public Welfare, Parts 160 (General Administrative Requirements), 162 (Administrative Requirements), and 164 (Security and Privacy)

C. Section 282.318, Florida Statutes, Enterprise Security of Data and Information Technology

D. Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

III. Supportive Data

A. 16 CFR., Section 681, Identity Theft Rules

B. 15 United States Code (USC) 1681, Credit Reporting Agencies, Congressional Findings and Statement of Purpose

IV. Signature Block with Effective Date

Signature on File — 1/22/2016
Jennifer Tschetter — Date
Chief Operating Officer

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. An information security and privacy program that is responsive and adaptable to changing environments, vulnerabilities, and technologies, affecting state information and information resources.

2. Documented information security and privacy policies, protocols, and procedures for each local entity, to include written local operating procedures for implementing, reviewing, and updating local information security policies, protocols, and procedures.

3. Documented procedures for monitoring compliance with the local information security and privacy policies, protocols, and procedures.

4. Documented procedures for developing and implementing corrective action plans.

B. Personnel

Director and Administrator of each Department division, office, CHD, and CMS area office, and other staff designated as responsible for developing and updating local information security and privacy protocols, procedures, and corrective action plans.

C. Competencies

1. Knowledge of federal laws, Florida Statutes, Florida Administrative Codes, departmental policies, protocols, and procedures, and industry standards, pertaining to information security and privacy.

2. Knowledge of department policies, protocols, and procedures related to security and privacy of information.

D. Areas of Responsibility

1. All Department Employees

    a) All members of the workforce are responsible for protecting Department data, resources, and assets in their possession.

b) All members of the workforce are responsible for immediately notifying their local Information Security Coordinator of any violation of Department security policies, or suspected/potential breach of security.

2. Information Security Manager (ISM)

The Information Security Manager shall administer the Department information security program. Responsibilities include:

a) The development, review, and updating of the Department information security and privacy policies, protocols, and procedures.

b) The development, review, and updating of the Department's strategic information security plan and associated operation information security plan.

c) The coordination of the Department information security risk management process.

d) The coordination of the Department Computer Security Incident Response Team (CSIRT).

e) The coordination of Information Technology Disaster Recovery planning in support of the Department Continuity of Operations Plan (COOP).

3. Department HIPAA Privacy Officer

The Department HIPAA Privacy Officer shall provide leadership for privacy oversight to ensure the Department complies with federal, state, and Department privacy requirements. Responsibilities include:

a) Participating in the development, implementation, and maintenance of policies, protocols, procedures, and corrective action plans related to privacy matters.

b) Provides counsel for privacy matters to the Department security program.

c) Provides consultation on information privacy awareness training to all members of the workforce.

d) Ensures the organization has and maintains appropriate consent and authorization forms, notice of privacy practices and materials

reflecting current organization, and legal practices and requirements.

e) Develops and implements information privacy risk assessments in coordination with the Department ISM and HIPAA Complaint Officer and conducts related ongoing compliance monitoring.

f) Works cooperatively with the local legal counsel, local privacy coordinators, and other applicable organizational units in overseeing client rights to inspect, amend, and restrict access to protected health information (PHI).

g) Initiates, facilitates, and promotes activities to foster privacy awareness within the organization and related entities.

h) Reviews all system-related information security plans throughout the organization's network to ensure the privacy of protected health information.

i) Maintains current knowledge of applicable federal laws, Florida Statutes, Florida Administrative Codes, departmental policy, protocols, and procedures; monitors advancements in technologies to ensure organizational adaptation and compliance in coordination with the Office of Information Technology (IT) and privacy coordinators.

4. Department HIPAA Complaint Officer

The HIPAA Complaint Officer shall serve as a point of contact for all questions regarding the content of the Notice of Privacy Practices, as well as all complaints regarding privacy violations. Responsibilities include:

a) Establishing and administering a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Department's privacy policies, protocols, and procedures.

(1) Violations categorized as a Category 2 per the Incident Reporting Policy, DOHP 5-6, must be referred to the Office of Inspector General for investigation.

5. Information Owner (formerly, Information Resource Owner)

Information Owners, must classify the data their organization possesses and must specify the security properties associated with each information set.

a) Information Owners served by networks shall prescribe sufficient controls to ensure that access to network services, host services, and subsystems are restricted to authorized users and uses only. Controls shall selectively limit services based upon user identification and authentication.

6. Local Information Security and Privacy Coordinators (ISPC)

Local ISPCs shall serve as liaisons for each local entity for security and privacy matters. They will work closely with the staff in their jurisdiction, other ISPCs, the ISM, and the HIPAA Privacy Officer to ensure a uniform approach to security and privacy. Responsibilities include:

a) Knowledge of respective statutes, administrative code, Departmental policies, protocols and procedures relating to information security and privacy.

b) Maintaining professional skills and competencies by participating in training and other professional development activities.

c) Coordinating the development and review of local information security and privacy procedures, at least annually.

d) Ensuring all members of the workforce in their jurisdiction have access to information security and privacy policies, protocols, and procedures.

e) Coordinating the procurement and dissemination of current information security and privacy awareness training materials consistent with Department policies and protocols.

f) Ensuring that all new members of the workforce have completed security and privacy awareness training within 30 days of employment and/or prior to accessing confidential information, whichever is earliest. Refer to the Acceptable Use and Confidentiality Agreement Policy, DOHP 50-10.2.

g) Coordinating an annual information security and privacy risk assessment for their respective entity.

h) Document a corrective action plan (CAP) for issues identified in the annual risk assessment, per the Risk Analysis Policy DOHP 50-10.8.

i) Enforce all information security and privacy policies.

j) Monitoring, at least annually, the list of staff authorized to access confidential information and facilitating corrections as appropriate. Refer to the Secured Areas and Physical Security Policy, DOHP 50-10.3.

k) Monitoring, at least annually, the assignment and maintenance of user credentials for all applications within their jurisdiction by reviewing the list of persons with access to electronically stored data and facilitating changes as appropriate.

l) Maintaining incident reports and documentation of resolution of all suspected and confirmed breaches of security and confidentiality.

m) Coordinating and monitoring corrective actions identified during the investigation of an incident or risk analysis. Refer to the Policy and Procedures on Incident Reporting, DOHP 5-6.

n) Assisting the local System Administrator with maintenance, training and annual testing of the site's Information Technology Disaster Recovery Plan. Refer to the Contingency Planning Policy, DOHP 50-10.9.

7. Local HIPAA Reviewing Officer

The Local HIPAA Reviewing Officer must be a licensed healthcare professional who holds a valid medical license in Florida and has been identified as a potential reviewing official for each of the covered entities. Responsibilities include:

a) Reviewing any individual's complaint on a decision to deny access to that individual's protected health information for the reasons specified in 45 CFR 164.524(a) (3).

(1) The reviewing officer cannot have been directly involved in the original decision to deny access.

8. Local Information Custodian and Key Custodian

The Local Information Custodian shall assist information owners in classifying data and specifying and implementing security controls to protect the integrity and accuracy of the data. Key Custodians must document and manage physical access to the secured area they are assigned and shall assist information owners with access control of information in designated secured areas. Key Custodians may be delegated authority to assist with Information Custodian duties, however this delegation must be documented. Responsibilities include:

a) Establishing procedures to ensure information is accessible only to authorized persons and maintaining access logs for information set(s).

b) Assisting owners in evaluating the cost-effectiveness of physical security controls and monitoring

c) Periodically reviews the access log for secured areas.

d) Implements and monitors techniques and procedures for reporting incidents.

9. Local IT Disaster Recovery Coordinator

Each local entity shall assign a Local IT Disaster Recovery Coordinator. In response to emergency events, this role may be required to work irregular hours, more than eight (8) hours per day, for extended periods (including weekends and holidays), at locations other than their official headquarters, and be required to perform duties in addition to those outlined in the employee's position description. Employees assigned to this role must be able to deploy to emergency sites with limited advance notice. Regional Disaster Preparedness Consultants shall not be designated Local IT Disaster Recovery Coordinator for any one office. Responsibilities include:

a) Planning and directing the detailed information technology activities before, during, and after a disaster.

VII. Procedure

Applicable policies, protocols and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Access to the internet, telephone, or email service is a privilege, not a right. All members of the workforce shall be held accountable for protecting information from unauthorized access, modification, destruction, disclosure, or improper use, and for safeguarding confidential information in accordance with federal laws, Florida Statutes, Florida Administrative Code, Department policies, and industry standards. All Department data, information, and technology resources shall only be used for official state business, except as allowed by the Department's policies. This includes information in any format or medium.

All members of the workforce shall receive mandatory information security and privacy awareness training prior to providing services to clients, accessing confidential information, accessing information technology resources, or within 30 days of employment start date, whichever is earliest. Additional training, based on job-specific duties or responsibilities, may be required.

All members of the workforce shall complete an annual refresher information security and privacy awareness training course.

The Department shall respect the legitimate proprietary interests of intellectual property holders and obey the copyright law prohibiting the unauthorized use or duplication of software. Only authorized information technology (IT) members of the workforce shall install software and hardware on Department systems. All software and hardware installed on Department systems must be approved by the Office of Information Technology (OIT).

An Acceptable Use and Confidentiality Agreement (Agreement), DH 1120, confirming the worker understands the requirements and penalties for failure to comply with information security and privacy policies, protocols, and procedures, shall be completed and signed by each member of the Department workforce. Members of the workforce should ask their management for any needed clarification prior to signing the Agreement.

Members of the workforce found to be in violation of these policies may be subject to disciplinary action, up to and including termination of employment, and/or legal action.

A. General

1. Supervisors may monitor computer use by direct observation, or reviewing work productivity and quality. If the supervisor observes, suspects, and/or was notified of an issue which requires additional information, they should contact their local Human Resource Management (HR) office. HR will contact the Department Information Security Manager (ISM) or the Office of Inspector General to request the information be provided and released, as appropriate.

2. Use of unapproved streaming media technologies requires prior written approval from the user's supervisor and the Information Security Manager (ISM) or delegate. Users may request approval through their supervisor using the Office of Information Technology Security Policy Exception Request Form.

3. Use of state resources constitutes consent to monitoring of activities with or without a warning.

    a. The workforce shall have no expectation of privacy when using Department resources.

    b. The Department may inspect any and all files stored on any Department network or local computer system, including removable media.

4. Only Department-owned or managed devices may be connected to the Department network. Exceptions require prior approval from the ISM.

5. Department devices (including computers, mobile devices, printers, etc.) will be configured according to OIT approved standards and guidelines.

6. Only Department-approved software shall be installed on Department-owned or Department-managed devices. This restriction does not apply to personally-owned devices approved for use in the Department's "Bring Your Own Device" (BYOD) program.

7. Illegal duplication of software is prohibited.

8. Users must immediately report suspected account compromises, including suspected computer malware (viruses, etc.) occurrences, to the local Information Security Coordinator and System Administrator or designee.

9. The workforce may use the Department's internet email access link for Department email access while away from the office with their supervisor's approval.

    a. Users may not configure a personal email client (e.g. Outlook, Thunderbird; Gmail) to connect to the Department email system without express authorization by the ISM.

    b. Included members of the workforce (eligible for overtime pay) must obtain prior approval for each use outside of their normal working hours and are required to account for all hours worked. Additional hours worked must be recorded as required by Department policy. Approval to use internet email access in no

way eliminates the requirement for prior approval for telecommuting in accordance with the Telework Policy, DOHP 60-24.

c. The workforce must ensure that the computer used for internet email access has up-to-date anti-virus software and current operating system security patches.

B. Computer Use

1. Members of the workforce will be given a user account to access Department IT resources. This access will be based on the documented need as provided by the appropriate hiring authority. The Department ISM or delegate has final authority regarding access to the Department network and IT resources.

   a) Access to Department IT resources is reserved for Department approved users.

   b) Department workforce shall have unique user accounts.

2. The local Information Security Coordinator, in coordination with supervisors, must regularly, but not less than annually, review and document the access privileges of their staff across all information systems using the User System Access Review (USAR) form in Appendix B and ensure access is appropriate to job responsibilities. Reviews must be submitted to the Security Administration Team by April 1, annually.

3. Users must never share account passwords or allow others to utilize their account credentials. Users are responsible for all activities occurring from the use of their account credentials.

   a) Department workforce is responsible for safeguarding their passwords and other authentication methods by not sharing account passwords, email encryption passwords, personal identification numbers, smart cards, identification badges, or other devices used for identification and authentication purposes.

   b) Passwords shall not be passed or stored in plain text. Passwords must be encrypted or secured by other means when delivered to users.

4. Department workforce shall be held accountable for their account activities.

   a) Audit records shall allow actions of users to be uniquely traced for accountability purposes.

b) User accounts must be authenticated at a minimum by a complex password.

(1) Department accounts will require passwords of at least ten (10) characters to include an upper and lowercase letter, a number, and a special character.

(2) Reference the Mobile Device Policy, DOHP 50-20 for Mobile Device Password requirements.

c) Department workforce shall immediately report suspected account compromises according to Department incident reporting procedures, DOHP 5-6.

d) Department workforce must log-off or lock their workstations prior to leaving the work area.

e) Workstations must be secured with a password-protected screensaver with the automatic activation feature set at no more than 10 minutes.

5. Department workforce must not disable, alter, or circumvent Department security measures.

C. Personal Use

1. Members of the workforce are permitted to briefly visit non-prohibited internet sites or use email and\or telephones for personal reasons during non-work hours (lunch period or before/after work) subject to the limitations contained within this policy. Local entities have the right to have local protocols and procedures that are more stringent. In the event of a conflict, the more restrictive security and privacy measures apply.

a) Personal use may be monitored and subject the employee to disciplinary action.

(1) Department workforce may access non-Department, browser-based email accounts such as Gmail, Yahoo, Outlook.com, etc.

(a) This privilege applies only to browser based email capabilities; users may not use Outlook, Outlook Express, or other PC-based software or plug-ins to access non-Department email.

(2) Usage must not interfere with the worker's job duties.

(3) Usage must not consume significant amounts of Department IT resources or compromise the normal functionality of the Department's systems.

(4) Personal use must not result in any additional cost to the Department and the Department accepts no responsibility for adverse incidents resulting from employee personal use.

b) Examples of acceptable internet/intranet sites are those dealing with health matters, weather, news, business or work-related topics, community activities, career advancement, and personal educational enrichment.

D. Unacceptable Uses

The prohibited activities listed below are examples and are not all inclusive. Department workforce performing any of these activities as part of their assigned job responsibilities must have written supervisor approval or these tasks must be identified in their position description.

1. Department IT resources must not be used for knowingly accessing, downloading, distributing, or participating in any of the following:

a) Any purpose which violates state or federal laws or rules.

(1) To include posting or sharing any confidential and/or exempt information on public facing or publicly accessible websites.

b) Personal profit, benefit, or gain.

c) Political campaigning.

d) Viruses, worms, Trojan horses, email bombs, etc., through willful intent or negligence.

(1) Note: Files downloaded from the internet must be scanned for viruses before use and/or distribution; no file received from an unknown source should be downloaded even if attached to an email message.

(2) Virus protection information can be found in Appendix D.

e) Harassing, intimidating, threatening, complaining, or otherwise annoying materials including, but not limited to, chain letters, thought/quote of the day, or motivational quotes.

f) Sexually explicit, pornographic, or vulgar material.

g) Inappropriate language or profanity, including, but not limited to obscene, racial, ethnic, hate-speech, or other discriminatory content.

h) Non-work related material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, or violence.

i) Unauthorized, non-work related access to chat rooms, news groups, political groups, singles clubs, dating services, computer hacker websites.

j) Solicitations for non-state-sponsored activities. This includes, but is not limited to, advertising the sale of a vehicle or other personal property; announcing the sale of cookies, candy, magazines, etc., on behalf of a school or organization; or announcing personal events (weddings, showers, or events not related to work).

3. Department workforce must not respond directly to the originator of an offensive email or forward the email to others. Recipients should report the communication to their supervisor, the Information Security Coordinator and, if necessary, to the Department Office of Inspector General.

4. Department workforce must not program Department email to automatically forward messages to a non-Department email address.

5. Department workforce must not create security breaches or otherwise disrupt network communications.

   a) Security breaches include, but are not limited to, unauthorized access of data not intended for the employee or logging into a server or account that the employee is not expressly authorized to access.

6. Any form of network monitoring or scanning used to intercept data is prohibited, except as authorized in the user's position description or in writing by the ISM.

7. Non-Department owned or managed devices shall not be connected to Department systems including, but not limited to, personal media players, thumb drives, printers, CDs, smart phones, etc.

8. Department workforce must not attempt to access information or resources without authorization.

9. Department workforce must not use Department IT resources for any activity which adversely affects the availability, confidentiality, or integrity of Department or state IT resources.

II. Authority

E. Chapter 71-A, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

F. Chapter 815, Florida Statutes, Florida Computer Crimes Act

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. An Acceptable Use and Confidentiality Agreement, provided in Appendix B, will be completed and signed by each member of the Department workforce prior to providing services to clients, accessing confidential information, accessing IT resources, or within 30 days of the employment start date; whichever is earliest. A new Agreement must be completed by members if there is a change in policy or a change in users' roles and responsibilities.

2. The Agreement shall be maintained by the local HR office.

3. Appropriate security controls are in place to mitigate risks of using information technologies.

4. Members of the Department workforce utilize IT resources in a manner that safeguards those resources.

A. Personnel

All members of the Department workforce including volunteers and contractors accessing Department data and information resources.

B. Competencies

1. Knowledge and skills to reasonably safeguard confidential and/or exempt information from any unauthorized use or disclosure.

2. Knowledge of federal laws, Florida Statutes, Florida Administrative Code, Department policies, protocols, procedures, and industry standards related to information security and privacy.

C. Areas of Responsibility

1. All members of the Department workforce with access to confidential information must sign Section A of the Agreement.

2. All members of the Department workforce having access to Department IT resources must sign Section B of the Agreement.

3. The signed Agreement must be maintained by the local HR office. This document shall be signed by the employee and witnessed by the employee's supervisor or designee.

4. All members of the Department workforce will have access to relevant Florida Statutes, Florida Administrative Code, Department policies, protocols, and procedures.

VII. Procedure

Standard Operating Procedures

VIII. Distribution List

All Department workers

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

The Florida Department of Health (Department) divisions, offices, county health departments (CHDs), and Children's Medical Services (CMS) area offices, must designate and maintain secured areas to ensure the security and privacy of information and information technology resources. Each designated secured area shall be documented in the local information security and privacy procedures.

A. General Secured Area

1. Secured areas must have a reliable locking system.

    a) Doors shall remain locked at all times, unless an authorized staff member is present.

    b) If an electronic locking system is used, a manual locking system must be in place in the event of a power outage.

2. Windows, walls, floors, and ceilings must not allow unauthorized access to the secured area.

    a) Electronic detection devices are acceptable alternatives to hard ceilings.

    b) Other barriers that are reasonable, such as metal screens, are also acceptable.

3. Access to secured areas shall be limited to a documented list of authorized personnel.

    a) Access logs must be maintained for each secured area.

    b) Access Control Lists (ACL) identifying authorized personnel shall be prominently placed at the entry way of each secured area. General use computer rooms, such as a training or 'resource room' are not required to have a posted ACL.

        (1) Personnel with access to secured areas shall be considered to be in a position of special trust and shall require Level 2 background screening.

        (2) Persons having temporary or occasional authorized access shall be escorted at all times by authorized personnel on the ACL.

(3) Persons having temporary or occasional authorized access, but are not on the list, must record their signature, data, time in and out, the purpose of entering the room, and description of any items taken from the secured area.

c) Documentation of the number of keys distributed for each secured area shall be maintained.

(1) Documentation must include the signature of the person receiving and returning the key.

(2) No key shall be provided for persons not on the list of personnel with authorized access.

B. Computer Rooms

1. Physical controls shall be appropriate for the size and criticality of the information technology resources within a secured area.

a) All non-IT staff must be accompanied by an authorized IT staff member when accessing a computer room.

b) Management reviews of physical security measures shall be conducted annually and whenever facilities or security procedures are modified or compromised.

c) New and remodeled Department computer rooms must be constructed so that they have reasonable protection against fire spread, water damage, vandalism, and other potential threats.

d) Information resources shall be protected from environmental hazards; in accordance with manufacturer's specifications.

e) All computers must be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers in accordance with Department information technology standards.

f) Policies and procedures will be implemented to document repairs and modifications to the physical components of the facility which are related to security.

X. Authority

A. Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

B. 45 Code of Federal Regulations (CFR), Public Welfare, Part 164.310 (a)(2)(iv) (Security and Privacy)

XI. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

XII. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

XIII. Definitions

See Appendix A

XIV. Protocol

A. Outcomes

1. All confidential information is maintained in a secure and confidential manner.
2. Client privacy is maintained.
3. Employee privacy is maintained.
4. The integrity of data is protected.
5. Access to confidential information is limited to those with a documented “need to know”.
6. Information and information technology resources are protected against alteration, disclosure, and destruction.

B. Personnel

All Directors and Administrators of Department divisions, offices, CHDs, and CMS area offices, as well as other staff designated with the responsibility of securing information for the purposes of protecting confidentiality, data integrity, and access.

C. Competencies

1. Knowledge of federal laws, Florida Statutes, and Florida Administrative Code, pertaining to physical security requirements, public records, exemptions from disclosure, and requirements for maintaining confidentiality of information.

2. Knowledge of Department policies, protocols, and procedures related to physical security, as well as security and privacy requirements of confidential information.

3. Knowledge of industry standards of information technology resource security requirements and practices.

D. Areas of Responsibility

1. The Information Security and Privacy Coordinator(s) is responsible for ensuring secured areas have reliable locking systems.

2. The information custodian is responsible for ensuring that the secured area has access limited to a documented list of authorized personnel.

3. A key custodian and an alternate key custodian are responsible for documenting and managing physical access to secured areas.

4. The System Administrator is responsible for the security of the computer rooms.

XV. Procedure

Applicable policies, protocols, and procedures.

XVI. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

XVII. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This

policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Each Department of Health (Department) division, office, county health department (CHD), and Children's Medical Services (CMS) area office, shall classify information and data sets of any format held in their custody. Local operating procedures shall be established to ensure information is classified correctly and is released only in accordance with federal and state laws and Department policies, protocols, and procedures. Information and data, made or received in connection with the transaction of official business, not classified as confidential, shall be classified as public.

Law changes affecting confidentiality of records will be applied to records in the possession of the Department when the specific law becomes effective whether or not otherwise addressed in this policy. Refer to 45 CFR 164.530(h)(2).

A. Public Information

Information and data that is not exempt from disclosure by federal law, Florida Statutes, or Florida Administrative Code is subject to personal inspection and copying by any person.

B. Confidential Information

Information and data which is exempt from disclosure by federal law, Florida Statute, or Florida Administrative Code shall be classified as confidential. Confidentiality laws primarily affecting the Department are as follows:

1. Personnel Records – Information maintained in personnel records are generally accessible to the public with certain exceptions as outlined in Chapter 119, Florida Statute.

    a) Social security numbers held by the Department of all current and former members of the workforce are confidential with the following exceptions:

        (1) When a current or former employee consents in writing to the disclosure.

        (2) When necessary for administration of benefits provided by the Department, such as:

            (a) Health benefits

            (b) Pension, retirement, or deferred compensation plans

(3) When necessary for the Department to perform its duties and responsibilities as prescribed by law, such as for completing Worker's Compensation forms.

(4) When required by federal or state law or a court order

2. Information, including but not limited to, the home address, telephone number, social security number, photographs, dates of birth, places of employment of the spouses and children, names and locations of schools and day care facilities attended by the children of the following:

a) Current or former justices of the Supreme Court

b) Judges, to include District Court of Appeal, Circuit Court, County Court

c) Current or former state attorneys, assistant state attorneys

d) Statewide Prosecutors, Assistant Statewide Prosecutors

e) Current or former human resource, labor relations, or employee relations directors, assistant directors, managers, or assistant managers of any local government agency

f) Active or former sworn or civilian law enforcement or firefighters

g) Current or former code enforcement officers

h) Department personnel whose duties are to support the investigation of child abuse or neglect

i) Department of Children and Family Services personnel whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, or other criminal activities

j) Servicemembers who served after September 11, 2001. This includes any current or former member of the Armed Forces of the United States and those who served in a reserve component or National Guard

3. Complaints and other records in connection with hiring practices, position classifications, salary, benefits, discipline, discharge, employee performance, evaluation, or other related activities are exempt from disclosure until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding

4. Medical information pertaining to a prospective, current, or former officer or employee is confidential and not disclosable unless the person or person's legal representative provides written permission or pursuant to court order. Refer to Section 119.071(4)(b)1.,Florida Statute.

5. Contracts

   Sealed bids, proposals, or replies received by the Department pursuant to a competitive solicitation are not discloseable until such time as the agency provides notice of an intended decision or until 30 days after opening the bids, proposals, or final replies, whichever is earlier. Refer to Section 119.071(1)(b)2,Florida Statute.

   Any financial statement that the Department requires a prospective bidder to submit in order to pre-qualify for bidding is not discloseable. Refer to Section 119.071(1)(c),Florida Statute.

6. Client Eligibility Applications

   All protected health information (PHI) contained in records relating to an individual's personal health or eligibility for health-related services held by the Department is confidential and exempt. Refer to Section 119.0712(1), Florida Statute and 7 CFR 246.26.

7. Computer Software

   Data processing software obtained by the Department under a licensing agreement that prohibits its disclosure and which software is a trade secret, as defined in Section. 812.081, Florida Statute, and agency-produced data processing software that is sensitive are exempt.

   a) The designation of agency-produced software as sensitive shall not prohibit an agency head from sharing or exchanging such software with another public agency. Refer to Section 119.071(1)(f),Florida Statute.

8. Regulatory Investigations – Health Professions and Occupations

   All information obtained during investigations of regulated health professions and occupations is confidential until 10 days after probable cause has been found or until the subject waives his or her privilege of confidentiality, whichever comes first.

a) The subject of the investigation may receive a copy of the patient record connected with the investigation if the subject agrees in writing to maintain the confidentiality of any information received. Refer to Section 456.073(10), Florida Statute.

9. Licensure Applications

All information submitted in an application for health profession and occupation license is a public record and subject to public inspection with the following exceptions

a) financial information

b) medical information

c) school transcripts

d) examination materials including questions, answers, papers, grades, and grading keys

10. Department of Children and Families (DCF)

The Department of Health and the DCF may share confidential information on any individual who is or has been involved in any program of both agencies. Legal documents must be present to confirm right of access. Refer to Section 381.0022, Florida Statute.

11. Disease Reporting

Medical information received by the Department identifying an individual for disease reporting, animal bite, or epidemiological research is confidential and only disclosable as necessary to protect public health. Refer to Section 381.0031, Florida Statute, and 45 CFR 160.203(c).

12. Immunization Registry

Records of child immunizations maintained in the state's registry are available to entities required by law to know a child's immunization history such as schools, licensed child care facilities, and licensed healthcare providers. Refer to Section 381.003(1)(e)3., Florida Statute, and 45 CFR 160.203(c).

13. Investigations – Child or Adult Abuse and Missing Child

Protected health information about child or adult abuse or missing children may be disclosed to an investigating law enforcement officer or

DCF investigator. Refer to 45 CFR 160.203(c), Sections 39.0132, 415.1045, and 937.025, Florida Statute.

14. Special Needs Shelter

The registry of persons with special needs is confidential and includes all information gathered concerning a person with special needs. Registry information is available to other emergency response agencies as determined by the local management director. Refer to Section 252.355(4), Florida Statute.

15. School Health Records

Health records maintained as part of the school health services plan is confidential pursuant to Sections 381.0055 and 456.057, Florida Statute, 20 United States Code Section 1232g, and 34 Code of Federal Regulations 99.31 through 99.33.

16. Vital Statistics

The release of vital statistic information, including but not limited to, birth, death, marriage, dissolution or marriage, and name change is confidential pursuant to Chapter 382, Florida Statute.

17. Women, Infants, and Children (WIC) Program

All client and vendor information from the federally sponsored Women, Infants, and Children (WIC) program is confidential and can only be disclosed, refer to 7 CFR 246.26:

a) To other government agencies providing services to WIC applicants for child abuse or neglect reporting

b) In response to subpoenas, court orders, and search warrants after local attorney review

c) As authorized by the applicant or vendor

18. Division of Disability Determination (DDD)

Disclosure of PHI in the possession of the Division of Disability Determination (DDD) in performance of its contract with the Social Security Administration (SSA) is exclusively controlled by the applicable federal laws and regulations for SSA and not otherwise addressed in this policy. Refer to Sections 5 USC 552 and 42 USC 1306.

C. Access to Confidential Information

Access to the health record and health information is limited to those with a documented “need to know”, such as:

1. Persons responsible for documentation and management of the patient’s care (nurses, doctors, nutritionists, etc.)

2. Other persons authorized by the agency (e.g. quality reviews, insurance reviews, or research)

3. Patient and/or their legal representative with the proper written authorization

Members of the workforce who are found to have accessed or modified a health record or health information outside of their assigned job duties will be subject to appropriate administrative and disciplinary action, up to and including dismissal.

D. Protection of Confidential Information

Confidential information in any format must be secured using appropriate administrative, technical, and physical safeguards.

1. The local Information Security and Privacy Coordinator(s) shall be granted access to review audit logs containing accountability details regardless of format.

2. Data sharing agreements and procedures shall be in place for sharing, handling, or storing confidential data with entities outside the Department.

3. Information with employee identifiers, client identifiers, or other confidential content shall not be left unattended or unsecured.

4. Computer monitors must be protected to prevent unauthorized viewing.

5. Consultations involving confidential information must be held in areas with restricted access.

6. Confidential information must be printed using appropriate administrative, technical, and physical safeguards to prevent unauthorized viewing.

7. Confidential information must be encrypted during transmission over any network not owned by the Department.

8. Telephone Information

a) Confidential information is discussed by phone only in areas where the conversation cannot be overheard.

b) Conversations held over cellular phones are not considered to be secure. Confidential conversations should be limited. The person called should be advised that the discussion is taking place on a cellular phone.

9. Mailing Information

a) A secured mail intake site must be used to receive incoming confidential mail.

b) Mailrooms and mailboxes must be secured to prevent unauthorized access to incoming and outgoing mail.

c) Double enveloping is required when mailing confidential or sensitive information. Only the Department's logo and required addresses should be included on the exterior envelope. No specific program should be identified. The outside envelope is addressed to the recipient. The inside envelope is marked confidential and specifies the recipient.

10. Facsimile Information

a) Confidential information may be faxed using appropriate administrative, technical, and physical safeguards. Protected health information may be faxed for the purpose of treatment, payment, and healthcare operations, or with specific authorization from the client.

b) Facsimile machines designated to receive or transmit confidential information must be maintained in a secured area.

c) Facsimile machines designated for transmitting confidential information must have the ability to generate activity reports or a call shall be made to confirm receipt.

d) A cover sheet marked "confidential" and containing the following paragraph must accompany all confidential transmissions:

"This transmission may contain material that is CONFIDENTIAL under federal law and Florida Statutes and is intended to be delivered to only the named addressee. Unauthorized use of this information may be a violation of criminal statutes. If this information is received by anyone other than

the named addressee, the recipient shall immediately notify the sender at the address or the telephone number above and obtain instruction as to the disposal thereof. Under no circumstances shall this material be shared, retained or copied by anyone other than the named addressee."

11. Electronic Mail (Email)

    a) Confidential information must be encrypted during transmission over any network not owned by the Department. If unencrypted email containing confidential information has been sent outside the Department network notify your Information Security and Privacy Coordinator immediately.

12. Clinic Procedures - General

    a) Telephones shall be answered in a manner that does not identify any clinic programs or services offered.

    b) Registration and financial eligibility determination interviews shall take place in an area that does not compromise client confidentiality.

    c) When necessary, only the first name or last name of the client shall be called in any clinic. It is preferred that a number system be used.

    d) Sign-in logs may be used in general clinic settings only. Information collected is restricted to client's first name or last name and arrival time.

    e) The exterior of the health record folder shall only contain "allergy alert" and "name alert" labels. The exterior of the folder should never indicate type of service, program or medical condition. If more than one clinical location exists, the medical home of the health record may be identified on the exterior of the folder. It is recommended that a confidentiality notice be included on the exterior of the file folder.

    f) Records shall not be stored in a manner that would identify diagnosis or services rendered.

    g) Clients shall not be left unattended in restricted areas.

13. Clinic Procedures - Appointment Reminders

a) Appointment reminders are discussed with the client during the first visit and the preferred method of contact is documented in the client's medical record. If the client has given consent to be contacted by phone or text message, staff may leave a message stating only the date and time of the appointment. Text messages shall only be sent from a number or system that does not receive replies other than system generated confirmation of receipt.

b) Client communications such as appointment scheduling and appointment reminders must be handled in a manner that does not compromise the client's confidentiality and must not identify specific services, programs or clinics.

c) Only the Department's logo should be included on the exterior envelope of mailed appointment reminder(s). No specific program should be identified. This restriction does not apply to documents enclosed in a sealed envelope or given directly to the client. Contact information includes only the date and time of the appointment and a contact number if rescheduling is necessary.

14. Maintaining Confidential Information - Field Security

a) Confidential information shall only be transported by persons authorized to do so in their position description or as authorized by law.

b) Confidential information transported must be secured using physical safeguards and not left unattended or in a visible area of the vehicle.

c) Department workforce must sign out all information removed from the secured area.

d) Sign-out documentation must be retained by the information custodian in accordance with the record retention and disposition schedule developed by the Department, Records Management Policy DOHP 250-2.

e) Confidential information carried into the field shall be limited to the minimum required to perform that day's responsibilities.

f) Prior permission must be obtained if information will not be returned by the close of the same business day and must be secured in a manner that does not risk the disclosure of confidential information.

E. Disclosure of Confidential Information

Confidential information shall not be disclosed without proper authority. It is the responsibility of each member of the workforce to maintain the confidentiality of information and data. Any member of the workforce disclosing confidential information shall ensure sufficient authorization has been received, the information has been reviewed and prepared for disclosure as required, and no revocation of the requesting document has been received.

Legal review shall be obtained prior to disclosing confidential information in response to a subpoena, court order, or law enforcement demand.

Local operating procedures shall be established to ensure that protected information is released only in accordance with these protocols.

1. Operations and Payment

   Patient medical information may be shared with outside entities for payment processing and operations provided the patient has completed the Initiation of Services form DH 3204.

   a) A Business Associate Agreement may be required pursuant to Department Information Security and Privacy Policy, Contract Providers and Business Associates, DOHP 50-10.7.

2. Protected Health Information Disclosure

   Health care practitioners and providers involved in the care or treatment of a client may share PHI without the client's authorization for the purpose of treating that mutual client. Refer to Section 456.057(7)(a), Florida Statute, and 45 CFR 164.506(c)(2).

   a) Proper authorization to disclose PHI must be obtained prior to disclosure.

      (1) Written Authorization to Disclose protected health information

         (a) When a parent, guardian, or other person legally authorized to consent for health care services on behalf of a minor, the PHI may be disclosed to them. Refer to 45 CFR 164.502(g)(3)(i).

         (b) When a minor consents for health care services, only the minor may authorize disclosure of the PHI. Refer to 45 CFR 164.502(d)(3)(A).

(c) Readily identifiable PHI will be disclosed as directed in the authorization signed by the client or legal representative. The authorization will expire in 12 months unless otherwise specified within the document. The following will require specific authorization:

(i) Disclosure is to another healthcare provider for Human Immunodeficiency Virus (HIV) diagnosis or treatment. HIV testing and results require a specific authorization from the client stating the HIV test result may be disclosed to a specific person or organization.

When the disclosure is made, it shall be accompanied by a statement in writing which includes the following or substantially similar language: "This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of such information without the specific written consent of the person to whom such information pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for this purpose." Refer to Section 381.004(2)(f), Florida Statute.

(ii) All information and records held by the Department or its authorized representative relating to known or suspected cases of sexual transmitted diseases (STD) require specific authorization to disclose. Refer to Section 384.29, Florida Statute.

(iii) All information and records held by the Department or its authorized representative relating to known or suspected cases of tuberculosis or exposure to tuberculosis require specific authorization to disclose. Refer to Section 392.65, Florida Statute.

(iv) When a client's psychiatric, psychological, or psychotherapeutic records are requested

by the client or the client's legal representative, the health care practitioner may provide a report in lieu of copies of the records. Upon a client's written request, complete copies of the client's psychiatric records shall be provided directly to a subsequent treating psychiatrist. Refer to Section 456.057(6), Florida Statute and 45 CFR 164.508(a)(2).

(v) Substance abuse service provider client records shall not be disclosed without the written consent of the client, unless it is needed to provide emergency medical care or services to the client. Refer to Section 397.501(7)(a), Florida Statute.

(2) Subpoena for Medical Records

The Department may disclose medical records in the course of any judicial or administrative proceeding (civil or criminal action) for which a subpoena has been received if:

(a) The Department receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to notify the client or client's legal representative that their records are being sought and may be disclosed.

(i) "Satisfactory Assurance" means the party requesting the medical records has provided written notice to the individual; the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection; the time for the individual to raise objections to the court has lapsed and no objections were filed; or all objections filed by the individual have been resolved by the court and disclosures are consistent with the resolution.

(ii) Public health investigatory records, HIV results, substance abuse service provider client records, and WIC records will not be disclosed in response to a subpoena. Refer to Section 456.057(7), Florida Statute, 45

CFR 164.512(e)(1)(iii)(A), and 7 CFR 246.26.

(3) Workers' Compensation Medical Records

Protected health information related to a workplace injury or illness specifically identified by the client as work-related is disclosable, upon the request, to the employer, employer's workers' compensation insurance carrier, an authorized qualified rehabilitation provider, or the employer's attorney without written authorization from the client. This disclosure is limited to records of services provided in the treatment of the specifically identified workplace injury or illness. Refer to Section 440.13(4)(c), Florida Statute. Records relating to HIV testing and results, WIC, substance abuse treatment, family planning, or other general medical records are not to be disclosed under this provision unless client injury or illness is clearly identified as work-related.

(4) Disclosure Record

Any disclosure of protected health information to a third party is to be documented showing the date, name, and address of the recipient, the purpose of the disclosure, and a general description of the information disclosed. This disclosure is authorized on the Initiation of Services, form DH 3204. Refer to 45 CFR. 164.528 and Section 456.057(12), Florida Statute.

(5) Client Access to Medical Record

A client may inspect and obtain a copy of their protected health information with the exception of:

(a) Psychiatric, psychological, or psychotherapeutic notes

(b) Other exceptions as defined in Section 456.057(7), Florida Statute, and 45 CFR 164.524(a)

(6) Patient Medical Records for Employees

Employees have the same patient privacy rights and the same procedures apply when accessing their protected health information. Refer to Section 456.057(7), Florida Statute, and 45 CFR 164.524(a).

(7) Deceased Individual's Medical Record

The protected health information of a decedent is confidential for 50 years following the death of an individual. The person's personal representative (the person under applicable law with the authority to act on behalf of the decedent or the decedent's estate) may be provided a copy of the records. With respect to family members or other persons involved in the care or payment for care prior to the individual's death, but who are not personal representatives, relevant protected health information may be disclosed to such persons, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the Department.

(8) De-identified Information

Medical information that has been de-identified and cannot be referenced back to any individual is not confidential and is available for public inspection and copying. 45 CFR 164.514 and Section 456.057(7)(a)4., Florida Statute.

3. Requirements for Protected Health Information Requests

Requests for PHI must contain the following core elements. Refer to 45 CFR 164.508(c)(1)(i-v):

a. A clear description of the information requested and associated patient identifiers.

b. The identification of the person or entity making the request.

c. The identity of the Department office having custody of the records.

d. The purpose of the request.

e. An expiration date or an expiration event. If no date or event is stated, expiration shall occur twelve months after authorized signature.

f. Signature of the individual and date. If the authorization is signed by a legal representative of the individual, proof of the legal representative's authority shall be provided.

g. Notice of the individual's right to revoke the authorization in writing for disclosures not yet having occurred.

h. Requests for patient medical records may use this format but may be exchanged on the simple request of one healthcare provider to another. Refer to Section 456.057(7)(a), Florida Statute, and 45 CFR 164.506(c). Efforts should be made to record any documents exchanged between healthcare providers of a mutual client for treatment purposes.

i. Specific authorization is obtained from client or legal representative before disclosure of HIV test results, psychiatric, psychological, or psychotherapeutic notes, WIC, and substance abuse service provider client records for a purpose other than treatment. Refer to Sections 381.004(2)(e), 456.057(6), 456.057(7) and 397.501(7)(a), Florida Statute, 45 CFR 164.508(a)(2); Section 397.501(7), Florida Statute, and 42 CFR Part 2 and 7 CFR 246.26, respectively.

4. Forms and Pamphlets

One pamphlet and two forms are utilized by the Department in its relation with the public for disclosure of confidential information and specifically patient medical information. The pamphlet is NOTICE OF PRIVACY PRACTICES, number: DH 150-741. The forms are INITIATION OF SERVICES, number: DH 3204; and AUTHORIZATION TO DISCLOSE CONFIDENTIAL INFORMATION, number: DH 3203. The pamphlet and forms are incorporated and authorized by this policy and can be located in Appendix B.

a. The Department Office of General Counsel shall maintain a reference list of federal laws, Florida Statute, and Florida Administrative Code relevant to Department confidential information.

b. The information custodian will maintain audit logs of access and updates to confidential information.

c. All members of the Department workforce shall be knowledgeable of the classifications of data/information and the proper handling of data/information per its classification.

d. Data backups must be locked in a secured area. Refer to Information Security Policy DOHP 50-10.10.

II. Authority

A. 45 Code of Federal Regulations (CFR), Public Welfare, Parts 160 (General Administrative Requirements), 162 (Administrative Requirements), and 164 (Security and Privacy)

B. Chapter 71-A, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

C. Section 282.318, Florida Statute, Enterprise Security of Data and Information Technology

III. Supportive Data

Federal and state laws, rules, and regulations referenced in this policy and Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. Security and privacy of client information is maintained.
2. Confidential information is disclosed only by authorized members of the workforce and only after proper authorization has been obtained.
3. Information that is exempt from public record disclosure is maintained in a confidential manner.

B. Personnel

All Department of Health members of the workforce designated as responsible for managing and disclosing confidential information.

C. Competencies

1. Knowledge of information classified as protected or exempt from public record disclosure in federal regulations, state laws, and rules pertinent to position responsibilities.

2. Knowledge of federal and laws, Florida Statutes, Florida Administrative Code, Department policies, protocols, and procedures related to maintaining the confidentiality of protected health information.

3. Knowledge of the appropriate elements that constitute a valid authorization to disclose confidential information.

4. Knowledge of the circumstances in which confidential information may be disclosed without the consent of the person to whom the information pertains.

5. Knowledge and skills to reasonably safeguard confidential information from any intentional or unintentional use or disclosure; ensure minimum necessary use and disclosure; and limit incidental uses and disclosures of the information.

6. Knowledge of patient's rights.

D. Areas of Responsibility

1. All Department Employees

   a) All members of the workforce are responsible for protecting Department data, resources, and assets in their possession.

   b) All members of the workforce are responsible for immediately notifying their local Information Security Coordinator of any violation of Department security policies, or suspected/potential breach of security.

   c) All members of the workforce shall be knowledgeable of the classifications of data and information and the proper handling of data and information.

2. The Office of General Counsel

   a) The Office of General Counsel is responsible for maintaining a reference list of all state and federal statutes and rules relevant to Department confidential information.

VII. Procedure

Applicable policies, protocols and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Each Department of Health (Department) division, office, county health department (CHD), and Children's Medical Services (CMS) area office, must have local information security and privacy policies and procedures that are consistent with the Department Information Security and Privacy Policy and protocols relating to clients' rights. Client rights are specified in Florida Statutes and the Health Insurance Portability and Accountability Act (HIPAA).

A. Notice of Privacy Practices

1. A "Notice of Privacy Practices" must be prominently displayed by each Covered Entity.

2. A "Notice of Privacy Practices" must be given to the client at the initial encounter with a Department Covered Entity and following each update to the notice, unless it is an emergency situation. Refer to 45 CFR 164.520(c)(2)(i)(A).

3. Receipt of the privacy notice shall be documented on the "Initiation of Services", form DH 3204, and kept in the client's medical record or maintained electronically. Refer to 45 CFR 164.520(c)(2)(ii).

B. Privacy Enforcement/Complaints

1. Complaints of inappropriate disclosure must be submitted in writing, as stated in the "Notice of Privacy Practices", to the Local Information Security and Privacy Coordinator, Department Inspector General, or the U.S. Department of Health and Human Services, Office of Civil Rights.

2. Local client complaints shall be reported to the Department HIPAA Complaint Officer.

3. The name, telephone number, and address of the Department HIPAA Complaint Officer must be provided.

4. The Local Information Security and Privacy Coordinator shall file an incident report per the Policy and Procedures on Incident Reporting, DOHP 5-6.

5. The Division of Administration, Bureau of Personnel and Human Resource Management, shall be responsible for developing and enforcing standard sanctions for employees who violate this policy and protocol.

C. Access to Protected Health Information

1. Access to PHI must be provided to a client or their legal representative upon written request with proper documentation.

    a. Clients or their legal representative may receive copies of their PHI.

    b. A reasonable copying charge may be established that includes labor and postage, if appropriate.

    c. Access may be denied and no review required if the PHI is exempt from access as specified in federal law and Florida Statutes.

    d. Clients have a right to receive a written accounting of disclosures of PHI to third parties for a minimum of the last six years.

2. Clients or their legal representative must be notified in writing within 30 days of the decision to permit or deny access. An extension of 30 days may be granted once, if the record is filed off premises.

3. Access to PHI will be denied when it may endanger the life or physical safety of the client or another person. Denial of access shall be determined by the healthcare practitioner.

    a. If access is denied, the client has the right to have the action reviewed by a licensed healthcare professional who is designated by the Department to act as the HIPAA Reviewing Officer who did not participate in the original decision to deny access. The client must be notified in writing regarding the decision.

D. Amendments to Protected Health Information

Clients or their legal representative have the right to request an amendment to their protected health information (PHI).

1. Requests to amend a record must be received in writing and include the reason to support the amendment.

2. Department must act within 60 days of the request and may have one 30 day extension if the client is advised in writing of the cause of the delay.

3. If the request to amend is granted, the Department must provide the amendment to any previous disclosure recipients identified by the client.

4. The request to amend can be denied if:

    a. The information was not created by the Department.

b. The information is accurate and complete.

c. The information would not be available for inspection under the right of access.

5. If the request to amend is denied, the client must be provided in writing the following:

a. The reason for the denial.

b. Directives in submitting a statement of disagreement to be filed in the record.

c. The request for amendment, the denial, and the statement of disagreement is released with any future disclosure(s). Process for filing such a statement consists of:

(1) All documents relating to the request for amendment must be filed in the client's PHI record.

(2) If the client is denied the right to amend the PHI, the Department HIPAA Privacy Officer must be notified of the action.

6. The Division of Disability Determination (DDD) must acknowledge receipt of a privacy act request within 20 working days of receiving a written request. If DDD has jurisdiction of the file and direct access by an individual to medical records about himself is expected to cause an adverse effect, DDD will ask the requestor to designate, in writing, a responsible person to receive the requested records. Social Security Administration is the official custodian of the records contained in the Certified Electronic Files. Requests for copies of an entire claim folder will be forwarded to Social Security Administration, as DDD does not have access to all systems that contain "official folder material."

E. Restrictions of Uses and Disclosures of Protected Health Information

Clients may request restrictions be placed on uses and disclosures of PHI.

While the Department is not required to agree to any restriction, the Department must honor any restrictions granted by not disclosing restricted information, except in emergency situations. Requests for restrictions shall be referred to the Local Information Security Privacy Coordinator for review and action.

F. Alternate Method of Communications

Clients may request alternate methods of communication and may change designation of methods of communication at any time.

1. Alternate methods of communication shall be documented in the medical record, noted in the clinical management system, and shared with all programs and departments that could contact the client.

2. If the alternate method of communication is accepted, all communication to the client should be by the method requested and approved.

   a. Communication includes billing information.

G. Florida Patient's Bill of Rights and Responsibilities

The client's privacy rights shall be respected consistent with providing adequate medical care and efficient facility administration pursuant to section 381.026, Florida Statute.

II. Authority

See Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A.

VI. Protocol

A. Outcomes

1. A "Notice of Privacy Practices" provided to each client by every Department division, office, CHD, and CMS area office designated as a Covered Entity.

2. A "Client Privacy Rights" prominently displayed in each Covered Entity's office/clinic.

3. Standard process for individuals to make complaints concerning the provisions of this policy and the Department's adherence to this policy including documentation of complaints and the disposition thereof.

4. Clients or their legal representative have the right to specific client rights such as access, amendments, and restrictions of their protected health information (PHI).

5. Client privacy maintained in accordance with federal laws, Florida Statutes, Florida Administrative Code, Department policies, protocols and procedures.

B. Personnel

All Department members of the workforce with access to PHI.

C. Competencies

1. Knowledge of federal laws, Florida Statutes, Florida Administrative Code, Department policies, protocols and procedures.

2. Knowledge necessary to coordinate the implementation of federal laws, Florida Statutes, Florida Administrative Code, Department information security and privacy policies, protocols, and procedures.

3. Knowledge related to security and privacy of PHI relating to client rights.

D. Areas of Responsibility

1. All Department Employees

   a) All members of the workforce are responsible for protecting Department data, resources, and assets in their possession.

   b) All members of the workforce are responsible for immediately notifying their local Information Security Coordinator of any violation of Department security policies, or suspected/potential breach of security.

VII. Procedure

Applicable policies, protocols and procedures.

VIII. Distribution List

Chief of Staff
Deputies

Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Health information maintained as a result of a public health activity is outside the jurisdiction of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

A. Protected health information (PHI) maintained in a public health disaster, emergency, communicable disease surveillance, or epidemiology investigations are exempt from HIPAA.

B. "Notice of Privacy Practices" is not required in the following:

1. Reportable diseases as specified in Florida Statutes.
2. Syndromic Surveillance and surveillance of communicable disease or disease outbreaks.
3. Epidemiology investigations of communicable disease outbreaks.
4. Locating contacts for communicable disease prevention.
5. Department Registries
6. Regulatory activities
7. Child Abuse Registries
8. Environmental Health Program investigations.
9. Reporting to Department of Children and Families (DCF) for Missing Child Investigation - statute requirement.
10. Community Health Screening.
11. Public health student screening.
12. Tobacco Free Florida Services
13. Women, Infants and Children (WIC) Program Services

C. Patient authorization is not required for information to be submitted to the following registries:

1. Tuberculosis (TB)
2. Sexually Transmitted Diseases (STD)

3. Human Immunodeficiency Virus (HIV)
4. Cancer/Tumor
5. Immunization
6. Vital Statistics
7. Brain and Spinal Cord Injury
8. Infant Death
9. Communicable Disease Reporting
10. Child Death Review
11. Trauma

II. Authority

See Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. Information related to public health events, disasters, and investigations is identified and maintained.

B. Personnel

All Department of Health (Department) members of the workforce designated to work with the public health programs and activities and staff assigned the responsibility of disclosing Public Health Information (PHI).

C. Competencies

1. Knowledge of applicable federal laws, Florida Statues, Florida Administrative Code, Department policies, protocols, and procedures.

2. Knowledge necessary to implement information security and privacy policies, protocols, and procedures.

3. Knowledge of policies, protocols, and procedures related to the privacy of PHI as it relates to public health activities and investigations.

D. Areas of Responsibility

1. All Department Employees

   a) All members of the workforce are responsible for protecting Department data, resources, and assets in their possession.

   b) All members of the workforce are responsible for immediately notifying their local information security coordinator of any violation of Department security policies, or suspected/potential breach of security.

VII. Procedure

Applicable policies, protocols and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was

revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Each Department of Health (Department) contract resulting in the contract provider having access to, or producing (as a result of contract services), confidential information shall include the standard contract language below requiring the provider to implement policy and procedures that maintain confidentiality and security of all data, files, and records, including client records related to the services provided pursuant to the contract.

> *Information Confidentiality and Security: The provider shall maintain confidentiality of all data, files, and records, including client records, related to the services provided pursuant to this agreement in accordance with applicable state and federal laws, rules, and regulations and any department program-specific supplemental protocols, which are incorporated herein by reference and the receipt of which is acknowledged by the provider upon execution of this agreement. The provider is required to have written policies and procedures ensuring the protection and confidentiality of Protected Health Information. The department reserves the right to review the provider's policies and procedures.*

Each contract provider accessing protected health information (PHI) must have a Business Associate Agreement with the Department.

A Business Associate Agreement shall also be required when the Department (as the Covered Entity) permits a business associate to create, receive, maintain, or transmit PHI electronically on behalf of the Department.

A Business Associate Agreement is not needed if the disclosure is to a Covered Entity for treatment of an individual or by a group health plan, Health Maintenance Organization, or health insurer.

Each outside entity requesting a network connection to the Department's network is required to enter into a third-party networking agreement with the Department, Appendix B, Standard Third-Party Networking Agreement.

All Department contracts involving information technology shall require that all hardware or software acquired as part of the contract shall either conform to Department standards or have an approved exception and have been approved through the Department's governance process.

II. Authority

A. Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. All applicable provider contracts with the Department contain the Information Confidentiality and Security clause.

2. Contract providers have written information security and privacy policies and procedures for maintaining confidentiality related to contract services.

3. The provider shall maintain confidentiality of all data, files, and records, including client records, related to the services provided pursuant to their contract(s) in accordance with applicable state and federal laws, rules, and regulations, and any program-specific supplemental protocols issued to or by the Department.

4. Compliance with all Health Insurance Portability and Accountability Act (HIPAA) requirements.

5. Completed third-party network connection forms for each secure network connection with all outside entities.

6. All information technology (IT) contracts are in compliance with the IT technical standards and the IT governance policies and procedures.

7. All contracts involving the disclosure of protected health information contain a Business Associate Agreement.

B. Personnel

Directors and Administrators of Department divisions, offices, county health departments (CHDs), and Children's Medical Services (CMS) area offices as well

as other staff designated responsible for contract management activities and information technology network staff responsible for establishing network connections to outside contractors.

C. Competencies

1. Knowledge of information considered confidential or exempt from public record disclosure in federal and state laws, rules, and regulations requiring specific actions to safeguard and any other specific contract requirements regarding security of confidential information.

2. Knowledge of the Department's information security policies, protocols, and procedures. Knowledge of any program-specific supplemental protocols that may apply to a specific contract(s).

3. Knowledge of the Department's information technology networking standards, current networking technologies, and security practices.

D. Areas of Responsibility

1. Each contract manager is responsible for the following activities related to the contracts for which they are the official contract manager:

   a. Identify the need for and participate in the development of Department program-specific supplemental protocols for information security and privacy.

   b. Ensure that the provider has any applicable Department program-specific supplemental protocols related to a particular contract's program services.

   c. Provide technical assistance to contract providers regarding any program-specific supplemental protocols related to security and privacy.

   d. Give the provider a copy of the Department's current Information Security and Privacy Policy.

   e. In conjunction with the Department's program monitoring plan and process for the specific program services purchased, review or ensure review of provider compliance with confidentiality requirements, including any Department program-specific supplemental protocols related to confidentiality. The scope, content, and frequency of the review are to be consistent with state and federal laws or rules, Department policy, and program-specific monitoring plans affecting the contracted program to be reviewed. It may be used as a self-assessment check by

providers and as a contract manager's risk assessment monitoring checklist. Program-specific supplemental protocols may be added to the contract provider risk assessment.

2. Each organizational unit's local Information Security and Privacy Coordinator and System Administrator or designee is responsible for providing technical assistance to the contract manager to support the technical assistance and monitoring activities of the contract manager.

3. Legal staff shall review contracts to ensure legal sufficiency and statewide uniformity for interpretation of confidentiality matters and provide guidance and opinions, as needed.

4. The Office of Information Technology shall review and approve all requests submitted by outside entities for third party networking connections. The agreement shall be executed before any new networking connections are installed.

VII. Procedure

Applicable policies, protocols, and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

An annual risk analysis must be conducted by each Department of Health (Department) division, office, county health department (CHDs), and Children's Medical Services (CMS) area office using the current Department Information Security and Privacy Risk Assessment Form.

A copy of the completed risk assessment, including related corrective action plans, must be filed with the Information Security Manager (ISM), be accessible to management, and must be retained for six years.

In coordination with the Agency for State Technology (AST), a comprehensive risk analysis of critical information resources must be conducted every three years.

A. Corrective Action Plans

1. Corrective action plans clearly identifying each finding, steps required to correct the finding, expected date of completion, and the individual(s) responsible for implementing and monitoring each action item shall be implemented for areas of non-compliance.

2. Corrective Action Plans shall be completed using the form provided in Appendix B.

3. Corrective action plans must be submitted to the Information Security Manager on a quarterly basis.

4. Corrective action plans shall be discussed with the individual(s) having the authority to make recommendations for improvement, implement corrective actions, and monitor corrective action steps.

II. Authority

A. Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

1/22/2016

Signature on File
Jennifer Tschetter
Chief Operating Officer

Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. Completed risks analyses in accordance with Chapter 282.318, Florida Statutes.

2. Documentation of security and privacy corrective action plans is confidential and not subject to public disclosure.

3. Corrective action plans are accessible to Department management.

4. Corrective action steps will be documented and monitored through final implementation by the appropriate manager.

5. The relative risk(s) of required corrective action is identified and prioritized accordingly in each corrective action plan.

6. Updated operating procedures reflecting changes as a result of the risk analysis findings.

B. Personnel

Directors and Administrators of Department divisions, offices, CHDs, CMS area offices, local Information Security and Privacy Coordinators, and other staff designated responsible for performing information security and privacy risk analysis and developing/implementing security and privacy corrective action plans.

C. Competencies

1. Knowledge necessary to coordinate or conduct information security and privacy risk analysis.

2. Knowledge of federal regulations, state statutes and rules, Department policies, protocols, and procedures pertaining to protected information.

3. Knowledge of information technology resources, security, privacy, and practices.

4. Knowledge of record management practices including storage, retrieval, and disposition.

D. Areas of Responsibility

The appropriate manager is responsible for ensuring that operating procedures are updated to reflect changes as a result of the corrective action plan.

VII. Procedure

Applicable policies, protocols, and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

Each Department of Health (Department) division, office, county health department (CHD), and Children's Medical Services (CMS) area office, must develop and adopt a written, cost-effective Information Technology Disaster Recovery Plan (IT DR Plan).

A. IT DR Plan

1. The IT DR Plan must identify critical functions, document practices for the backup, storage, and retrieval of electronically stored information in the event of a disaster, whether it is man-made or natural.
2. The IT DR Plan shall be updated and tested at least annually to ensure that the plan documentation is kept up-to-date and that the plans continue to be relevant and effective.

    a. Each test must be followed by any necessary documentation updates and a brief written report to management and Central Office, Office of Information Technology (OIT) detailing the results of the test and remedial actions that will be taken.

3. The IT DR Plan shall be incorporated into the local Continuity of Operations Plan (COOP) as required by federal law, Florida Statutes, and Florida Administrative Code.

B. Data Backup

1. All Department personal computer user data shall be stored on a network shared drive or OneDrive.

2. Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or shall be backed up regularly with a current copy stored at an off-site location.

3. Servers and other multi-user systems shall be cataloged and backed up periodically.

    a. Backups must be stored off-site.

4. Department systems and machines are to be backed up according to the following guidelines:

    a. If the system supports more than one individual and contains data that is critical to the day-to-day operations of the Department, backup is required weekly.

b. If the system is used to support job-related functions and contains key data critical to the day-to-day operation of that job, backup is required weekly.

c. If the system is primarily used as a personal productivity tool and contains no data that would be classified as job or departmental in nature, backup is at the discretion of the individual user.

d. Nothing in the time frames for periodic backup restricts the generation of more frequent backups. For example, if hurricane warnings have been announced or there is a reason to suspect a threat to the integrity or reliability of the system involved, an immediate backup is advisable.

5. The Department requires the use of at least two (2) sets of backup storage media (tapes, CD-ROMs, etc.) to be used in rotation, one of which should be stored offsite, at a separate, secure, accessible, and fireproof location at least several city blocks away from the system being backed up.

6. All backup computer media (magnetic tapes, flash storage, optical disks, etc.) stored off-site must be physically protected against unauthorized access and other common mishaps like water or fire damage.

7. All computers containing electronic PHI shall be backed up, when feasible, prior to movement of equipment, per Health Insurance Portability and Accountability (HIPAA) requirements.

C. Third-Party Offsite Storage

If a third-party vendor is contracted to perform offsite storage, the following conditions should be met:

1. The backup media must be stored in a physically secure fashion to protect them from common mishaps like water damage and fire damage.

2. The media must be stored either in an encrypted format or in their own secured box inaccessible to unauthorized members of the workforce.

3. The vendor must be made aware of any handling requirements of the media.

4. The vendor must submit to periodic audits to ensure they maintain compliance with all storage requirements.

5. If electronic protected health information (PHI) is included on the backup tapes, the vendor will sign a written Business Associate Agreement stating that they understand the regulations and agree to maintain the security and privacy of the information stored on the media according to Department requirements.

II. Authority

A. Public Law (PL), 104-191, Health Insurance Portability and Accountability Act of 1996

B. Public Law (PL), 111-5, American Recovery and Reinvestment Act of 2009

C. 45 Code of Federal Regulations (CFR), Public Welfare, Parts 160 (General Administrative Requirements), 162 (Administrative Requirements), and 164 (Security and Privacy)

D. 16 CFR., Section 681, Identity Theft Rules

E. 15 United States Code (USC) 1681, Credit Reporting Agencies, Congressional Findings and Statement of Purpose

F. Section 282.318, Florida Statutes, Enterprise Security of Data and Information Technology

G. Chapter 71A-1.012, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards (Contingency Planning)

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. Availability, integrity, and confidentiality are maintained for essential Department operations, including the supporting technology and information resources.

2. Availability, integrity, and confidentiality of Department information is maintained.

B. Personnel

1. All Department divisions, offices, CHDs, and CMS area offices, as well as other staff designated with the responsibility of the following:

   a. Contingency planning for the continuity of business operations and disaster recovery (DR) of the information technology (IT) function.

   b. Staff providing essential information systems must backup information to ensure continued availability in the event of a disaster while also protecting confidentiality and data integrity of Department information.

C. Competencies

1. Knowledge of federal laws, Florida Statutes, Florida Administrative Code, Department policies, protocols and procedures, and industry standards pertaining to security, contingency planning, business continuity planning, and DR planning.

2. Knowledge of established Department policies, protocols, and procedures related to security, contingency planning, business continuity planning, and DR planning.

D. Areas of Responsibility

1. Department Managers:

   a. Determine all data, software, and IT resources essential to the continuity of Department operations.

   b. Prepare, periodically update, and annually test a DR plan that will allow all critical IT and communication systems to be available in the event of a loss.

c. A standard process for developing and maintaining both business contingency plans and computer contingency plans must be documented and maintained by the Department's COOP coordinator.

2. The Office of Information Technology:

a. Determine DR, or COOP-IT, planning and plan documentation standards, as well as for coordinate the Central Office DR planning and testing.

3. Local IT DR coordinators, with the assistance of regional disaster preparedness consultants, local Information Security and Privacy Coordinators, and other local IT staff:

a. Coordinate the local DR planning and testing functions, using the planning process and plan documentation standards established by the Office of Information Technology (OIT). The planning process should include the following areas:

(1) Identification and prioritization of critical business functions.

(2) Identification of risks facing the organization.

(3) Assessment of the potential impacts of various types of emergencies and disasters.

(4) Identifying and assigning responsibility for handling emergencies and disasters.

(5) Determination of critical applications and technical support services which support the critical business functions.

(6) Identification of data files and programs that should be backed up and stored off-site.

(7) Documentation verifying that the backup schedule is adequate.

(8) Assurances that all required documentation and other records stored off-site are kept current and complete.

(9) Pre-positioning of critical assets off-site, including Take-Home Kits or Drive-Away Kits containing essential supplies, forms, and files.

(10) Arrangements for operating at an alternate location(s) if the primary site is rendered inoperable.

(11) Detailed plans for transition to an alternate operating site(s) and for resumption of normal processing functions.

(12) Documentation of procedures and processes for recovery of all essential functions and applications.

(13) Education of staff and coordination of periodic testing of plans to practice the recovery procedures.

4. Information custodians

(1) Assist in the development and implementation of the Department's contingency planning and testing process.

VII. Procedure

Applicable policies, protocols, and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

I. Policy

The confidentiality, integrity, and availability of the Department of Health's (Department) resources must be protected, managed, and operated effectively to ensure a reliable IT infrastructure. Measures must be taken to ensure that Department networks remain available and secure.

Deviation from this policy requires written approval from the Department Information Security Manager (ISM).

A. Information Technology Workers – to include System Administrators and other designated staff

1. A background investigation, using at a minimum, Level 2 screening standards and disqualification criteria shall be conducted for all information technology workers and other positions of special trust as set forth in Section 110.1127 and Chapter 435 Florida Statutes.

2. On-going training shall be provided for information technology workers to ensure competency in both technical and security aspects of their positions.

B. Information Technology Resources

1. Access to IT resources shall be restricted to authorized users and uses only.

    a. The Department network shall be monitored for unauthorized devices, users, and uses.

    b. Audit records must allow actions of users to be uniquely traced to those users so they can be held accountable for their actions.

    c. Procedures to review records of information system activity, such as system audit and security logs, shall be implemented.

2. Procedures to track Department IT resources and associated owners and custodians must be implemented.

3. Information technology resources shall be sanitized by overwriting or degaussing media prior to reassignment, surplus, or disposal.

    a. Destruction of media is an acceptable method when computer equipment is planned for surplus and overwriting or degaussing media is not possible.

C. Information Technology Hardware and Software Standards

1. Standard hardware and software for use at the Department shall be specified.

    a. A list of standard hardware and software must be maintained, reference the Technology Reference Model.

2. Only hardware and software that has been approved as a standard by the Department shall be permitted.

    a. “Non-standard” hardware or software may be approved for use in specific circumstances by following the Information Resource Request process.

3. Risk assessments/feasibility studies shall be conducted prior to a new technology being approved or an existing technology being modified. This requirement does not apply to simple textual content changes in an application.

4. Standard configurations used to harden IT resources, including the requirement that vendor supplied defaults for system passwords and other security parameters are changed, shall be specified.

    a. Newly created or reset passwords for all systems and accounts shall be auto-generated specifically for each system and account.

    b. Passwords shall be encrypted while in transit and at rest (in storage) using Department approved encryption algorithms.

    c. IT resources must be configured to lock out a user ID after no more than five unsuccessful login attempts.

5. Administration of hardware, software, or applications performed over a network must be encrypted, where technology permits.

D. Access Control

1. Access to data and information systems must be controlled to ensure only authorized individuals are allowed access to information and that access is granted upon a “need-to-know” basis only.

2. User accounts shall be requested based on access needed and not be requested to mirror another user account.

3. User accounts shall be deleted within 30 days of employment termination, non-use of account for 60 consecutive days, or under direction of a

manager or Personnel and Human Resource Management's notification of a security violation. The 60 day limit shall not apply to the accounts of users who are in an authorized leave status.

4. Service accounts must be maintained in a manner that protects IT resources.

    a. Service accounts shall not be used for interactive sessions.

5. Administrative accounts, to include local administrator permissions, shall be restricted to members of the IT workforce who are authorized based on an IT position title, documented job duties and responsibilities requiring administrative rights, and who have received appropriate technical training.

    a. Administrative accounts shall be a secondary account and not be used as a primary user account.

    b. Procedures shall be established to ensure accounts with admin rights are created, maintained, monitored, and removed in a manner that protects IT resources.

    c. The ISM or delegate shall authorize each administrative account prior to creation and will review and reauthorize all administrative accounts annually.

    d. Administrative account activities must be traceable to an individual.

6. Remote Network Access

    a. Requests for remote access to the Department network will be made online to the IT.

    b. Remote access to the Department network is for use by approved Department workforce for business use only.

    c. Remote access client connections may not be shared.

    d. Remote access client requests will be signed by the worker's supervisor attesting that he/she has reviewed with the requestor the applicable Department policies including information security and privacy, computer use, overtime and compensatory time, and telecommuting; the Director or Administrator of the unit accepting associated financial obligations; and the local System Administrator attesting that all information on the form is accurate.

e. Users not part of the Department workforce with a valid Department-approved business need may be granted remote access to specific Department information technology resources by the ISM or designee.

f. The Security Administration Team will implement procedures to obtain required information and agreements from non-Department entities that require remote access to the Department network including but not limited to Third Party Network Connection Requests and Third Party Networking Connection Agreements.

E. Software Application Security Requirements

Software applications must be designed and configured with proper security controls in accordance with the National Institute of Standards and Technologies (NIST) Risk Management Framework (RMF) and secure coding best practices.

System components, processes, and software shall be tested frequently, but at least annually, to ensure implemented security controls remain effective.

1. Procedures to ensure application security is addressed throughout the application procurement process and/or application development lifecycle shall be developed.

2. Any third-party application that requires Department data be stored on non-Department servers must be approved for use by the ISM or delegate.

3. The application owner is responsible for defining application security-related business requirements.

4. The application development team shall implement appropriate security controls to achieve the security requirements of the application owner.

5. The application development team shall implement appropriate security measures to minimize risks to Department information technology resources.

6. A final application security review must be approved by the application owner, ISM or designee, and Chief Information Officer before a new application or technology is placed into production.

7. Each application or system with a Federal Information Processing Standards (FIPS) 199 categorization of moderate impact or higher shall have a documented system security plan.

a. System security plans must document the controls necessary to protect production data in the production infrastructure and copies of production data used in non-production infrastructures.

b. System security plans are confidential per Section 282.318, Florida Statute.

c. System security plans shall be made available to the Information Security Manager or designee.

8. The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

9. Application security documentation shall be maintained by the Department and be available to the ISM upon request.

F. Confidential Data and Software Applications

1. Access to confidential information, access to applications containing confidential data, and data sharing between applications, will be as authorized by the application owners.

2. Information owners will document their procedures for granting access to state information resources.

3. The Department will implement procedures to establish accountability for accessing confidential applications.

4. The Department will implement procedures to establish accountability for modifying confidential data.

5. Production exempt, or confidential and exempt data shall not be used for development.

6. The ISM or other authorized members of the workforce will be granted access to review audit logs containing accountability details.

G. Wireless Networks

Only Department owned or managed devices may be connected to the Department's internal network. Exceptions must be granted in writing by the ISM. Non-Department owned or managed devices may, with approval, connect to the Department's 'guest' wireless network.

1. Only OIT-approved wireless devices, services, and technologies will be used when connecting to the Department network.

2. The Office of Information Technology will manage all Department wireless access points.

3. Department wireless access points shall be tracked by the Department.

4. The Department shall monitor for unauthorized access points and immediately remove any that are discovered.

5. Department wireless devices must be configured and maintained according to Department standards.

6. Wireless access into the Department network must require user authentication meeting the Department security standard of EAP-PEAP/WPA2-Enterprise.

7. Remote users requiring access to internal Department resources must utilize a Department approved remote access solution (e.g. VPN, Remote Access Point (RAP), Unified Access Gateway (UAG)).

   Example 1: Johnny needs to access a secured shared folder on an internal file server from a hotel using the provided unsecured wireless connection. To access this file, Johnny must authenticate with his network credentials (e.g. SmithJR); therefore Johnny must use a Department approved remote access solution such as VPN.

   Example 2: Sally is awaiting an important confirmation email and needs to check her Office 365 email from the hotel using the same unsecured wireless connection. Sally can access Office 365 directly from the internet using her email address (Sally.Smith @flhealth.gov) as her id; therefore, Sally is not required to utilize a Department approved remote access solution.

H. IT Change and Release Management

1. The development infrastructure, test infrastructure, and production infrastructure shall be physically or logically separated.

2. The Change Management process must be used for new systems and applications, modifications to existing systems and applications, and deletion of systems and applications.

3. The Change Management process shall include a verification process ensuring compliance with Department standards and hardening

configurations including but not limited to vulnerability assessments for Department servers and applications.

4. Changes to the production environment must be approved by the Change Advisory Board before implementation to ensure they have been tested and documented.

I. Patch Management

1. A patch management process for information technology resources must be implemented.

2. Critical patches and all other security patches must be deployed within one working day of the conclusion of patch testing, but not later than two weeks following patch release without the approval of the ISM.

J. Malware Control

1. All Department computer systems must have current and up-to-date Department standard anti-malware software capable of detecting, removing, and protecting against all known types of malicious software.

2. Computer systems infected with malware shall be removed and remain off the Department network until they have been cleaned.

K. Network and Perimeter Security

1. Network perimeter security measures must be implemented to prevent unauthorized connections to Department information technology resources.

2. Department configuration standards for Department firewalls shall be established by the Office of IT.

    a. Firewall and router configuration standards must be tested upon changes in equipment or software or software configurations and must be reviewed at least every six months.

II. Authority

See Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

III. Supportive Data

Federal and state laws, rules, and regulations referenced in Appendix C, Confidentiality Statutes, Rules and Federal Regulations.

IV. Signature Block with Effective Date

Signature on File	1/22/2016
Jennifer Tschetter Chief Operating Officer	Date

V. Definitions

See Appendix A

VI. Protocol

A. Outcomes

1. IT infrastructure and members of the IT workforce are managed appropriately and effectively.

2. Written local operating procedures for implementation of IT issues.

3. Integrity of Department resources is maintained and IT resources are protected against unauthorized access, alteration, disclosure, or destruction.

4. Confidentiality is maintained.

5. Availability of IT resources is maintained.

6. Appropriate security measures are implemented to mitigate security risks to an acceptable level.

7. Software applications obtained, purchased, leased, and/or developed provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other IT resources.

B. Personnel

Directors and Administrators of Department divisions, offices, CHDs, and CMS area offices, System Administrators, Information Security and Privacy Coordinators, IT members of the workforce, and other staff designated responsible for operating, developing, administering, or managing Department IT resources and staff.

C. Competencies

1. Knowledge of federal laws, Florida Statutes, Florida Administrative Code, Department policies, protocols and procedures, and industry standards, related to security and privacy of information.

2. Knowledge of information technology resource security requirements and best practices.

3. Knowledge and skills to apply and maintain technical information security policies, protocols, and procedures.

D. Areas of Responsibility

1. Information Technology Workforce –System Administrators and delegated staff.

   a. The OIT will document minimum qualifications relative to training and experience for IT members of the workforce.

   b. The OIT is responsible for publishing protocols and procedures for the sanitization of equipment.

   c. IT members of the workforce will be granted access to Department information technology resources based on the principles of “least privilege” and “need to know.”

   d. The Department will implement controls to ensure access to information technology infrastructure resources is restricted to authorized users and uses.

   e. The Department will ensure separation of duties, so no individual has the ability to control an entire process.

   f. The Security Administration Team will develop and administer the patch management process for security patches of Department enterprise software.

   g. The Security Operations Response Team will implement the patch management process for security patches of Department enterprise software.

   h. System Administrators will ensure approved patches are applied within the designated timeframes.

   i. System Administrators will ensure that patches for non-standard IT resources, ITSW approved exceptions, are tested and applied when appropriate.

j. System Administrators will ensure anti-malware software is maintained on Department information technology resources.

k. System Administrators will ensure malware-infected computer systems are removed from the network until they are cleaned.

l. System Administrators will ensure computer equipment is sanitized properly by using software that ensures no data remains.

(1) Deletion of files is not an approved method of sanitization.

m. System Administrators, with their local property custodian, will ensure documentation of IT resource reassignment or surplus is updated in asset management records in accordance with the Management of State Property Policy, DOHP 250-11.

n. The Security Operations Response Team will perform configuration of Department personal firewalls used for employee remote access.

o. Unauthorized peer-to-peer traffic is prohibited.

p. The Office of IT will administer all Internet-facing Department servers (i.e., Demilitarized Zone – DMZ – servers).

q. All Department offices and programs shall utilize the IT web hosting services as outlined in the Department Information Technology Internet Web Hosting Policy, DOHP 50-16.

r. User password management shall only be performed in accordance with approved user password management procedures and utilizing only approved user password management tools.

s. The Security Operations Response Team will be granted access to review audit logs containing account activity details.

VII. Procedure

Applicable policies, protocols and procedures.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors

Bureau Chiefs
County Health Department Directors and Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The January 2016 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007, April 2010, and June 2015. The Office of Information Technology's Security Administration Team Manager is responsible for this policy.

Definitions for the Information Security and Privacy Policy Manual

Access - To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any information or system resource.

Authorization - Access privileges granted to a user, program, or process or the act of granting those privileges, or a person's written permission to use or disclose his or her personally identifiable health information for purposes of treatment, payment or health care operations or other designated purposes.

Availability - Ensuring that authorized users have access to information and associated assets when required. The security goal that generates the requirement for protection against intentional or accidental attempts to perform unauthorized deletion of data or otherwise causes a denial of service of system resources.

Business Associate - A person or entity who on behalf of the department performs or assists in the performance of a function or activity involving the use or disclosure of Protected Health Information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and reprising; or any other function or activity regulated by the HIPAA privacy rule.

A person or entity who on behalf of the department provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Department, where the provision of the service involves the department business associate. A covered entity may be a business associate of another covered entity. DOH workers are not considered to be DOH business associates.

Comprehensive Risk Analysis - See Risk Assessment.

Confidential Information - Information that is exempted from disclosure requirements under the provisions of applicable state and federal law, e.g., the Florida Public Records Act 119.07 *F.S.*

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Ensuring that information is accessible only to those authorized to have access.

Consent - Voluntary permission granted by a patient to a healthcare provider allowing the provider to administer care and/or treatment or to perform surgery and/or other medical procedures.

Contingency Plan - A plan for emergency response, back up operations, and post-disaster recovery in a system as part of an information technology security program to ensure availability of critical system resources and facilitate continuity of operations in an emergency situation. Refer to the Disaster-Preparedness Plan.

Continuity of Operations Plan (COOP) - Continuity of Operations Planning for government functions. This specifies that all mission essential government functions will be operational within twelve hours of an emergency and remain operational for up to 30 days, before returning to normal operations. Each DOH division, office, county health department, Children's Medical Services area office and the A.G. Holley Hospital will have a COOP plan.

Continuity of Operations Plan for Information Technology (COOP-IT) - The information technology disaster recovery plan to support the organization's COOP.

Control - Any action, device, policy, procedure, technique, or other measure that improves security.

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 - (1) A health plan, (2) A health care clearinghouse, (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by [HIPAA Privacy Rule] this subchapter, 45 CFR 160.103.

Critical Information Resources - The resources determined by DOH management to be essential to the DOH's critical mission and functions, the loss of which would have an unacceptable impact.

Custodian - See Information Custodian

Data Encryption Algorithm (DEA) - A symmetric block cipher, defined as part of the United States Government's Data Encryption Standard. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

Data Encryption Standard (DES) - A United States Government standard (Federal Information Processing Standard 46-3) that specifies the data encryption algorithm and states policy for using the algorithm to protect data.

Data Integrity - The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

Data Security - Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Department of Health (Department) - All Department of Health divisions, offices, county health departments, and Children's Medical Services area offices.

Disaster Preparedness Plan (or Continuity of Operations Plan) - An effort to ensure the continued performance of minimum essential functions during a wide range of potential emergencies. An operational and tested information technology continuity plan should be in line with the overall DOH disaster-preparedness plan and its related requirements and take into account such items as criticality classification, alternative procedures, back up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fallback and resumption plans, risk management activities, assessment of single points of failure, and problem management. Provisions should be documented in the plan and reviewed to establish back up and off-site rotation of non-critical application software and job execution language libraries, data files, and systems software to facilitate restoration following recovery of critical applications.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Encryption - Cryptographic transformation of data (called plaintext) into a form (called cipher-text) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: a key value that varies the transformation and, in some cases, an initialization value that establishes the starting state of the algorithm.

End User - A system entity, usually a human individual that makes use of system resources, primarily for application purposes as opposed to system management purposes. This includes State members of the workforce, contractors, vendors, third parties, and volunteers in a part-time or fulltime capacity.

Federal Information Processing Standard (FIPS) - A federal standard issued by the National Institute of Science and Technology

Governance - The formal structure established within the Department of Health to facilitate information technology planning, policy and procedure development, prioritization, and project monitoring. See the Information Technology Governance Policy, DOHP 50-3.

HIPAA Privacy Compliant Officer - The department's Inspector General functions as the DOH Privacy Compliant Officer and serves as a focal point for all complaints of privacy violations. Responsibilities may be found in DOHP 50-10a.

HIPAA Privacy Officer - The individual in the department who serves as the HIPAA privacy consultant and provides leadership for the department's implementation and administration of the HIPAA privacy law. Responsibilities may be found in DOHP 50-10a.

HIPAA Reviewing Officer (physician) - A licensed health care professional who has been assigned the responsibility of Reviewing Official for each of the covered entities in the department. Their responsibilities are to review HIPAA privacy complaints against that site;

however, they are not required to be located administratively at the site. Responsibilities may be found in DOHP 50-10a.

HIPAA Security Officer - The individual who has been assigned the responsibility for the department's implementation and administration of the requirements of the HIPAA Security Rule in the department's data and information technology security program. Responsibilities may be found in DOHP 50-10a.

Identifiers - Identifiers include the following: (A) Names; (B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older and; (D) Telephone numbers, fax numbers, electronic mail addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers, Biometric identifiers, including finger and voice prints, full face photographic images and any comparable images, and any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and 45 CFR 164.514(b)(2).

Incident Response Plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information system(s).

Individually Identifiable Health Information - 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.

Information Custodian (formerly, Information Resource Custodian) **-** DOH worker(s) responsible for assisting information owners in classifying data and specifying and implementing the technical mechanisms required to enforce policy to a degree of certainty required, based on a comprehensive risk analysis that considers the probability of compromise and its potential operational impact.

Information Owner or (formerly, Information Resource Owner) – Official, typically a DOH manager, with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal..

Information Resources or **Information Technology Resources** - Data; automated applications; and any transmission, emission, and reception of signs, signals, writings, images, and sounds of intelligence of any nature by wire, radio, optical, or other electromagnetic systems. It includes all facilities and equipment owned, leased, or used by all agencies and political subdivisions of state government, and a full-service information-processing facility offering hardware, software, operations, integration, networking, and consulting services.

Information Security Alert - A notice sent by state agencies pursuant to Chapter 60DD-2.006(6) (b), *F.A.C.*, regarding potential information security abnormalities or threats.

Information Security Manager (ISM) - The person designated to administer the DOH's information resource security program and plans in accordance with Section 282.318(2)(a)1, *F.S.*, and the DOH's internal and external point of contact for all information security matters.

Information Security and Privacy Coordinator - An individual in each DOH division, office county health department, Children's Medical Services area office, and the A.G. Holley Hospital who has been assigned the responsibility for the development and implementation of local procedures to carry out the requirements in the department's security and privacy policies, protocols and program.

Information Security Program - A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, whose purpose is to support the DOH's mission and establish controls to assure adequate security for all information processed, transmitted or stored in DOH automated information systems, e.g., Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information Set - A collection of information covering the same topic, or intended for the same purpose. Also referred to as a type of information. Examples of types of information, or information sets included: medical records, purchasing records, data sets, and personnel files.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information Technology Standards Workgroup (ITSW) - An internal committee which reviews and establishes IT standards for the Department of Health. The workgroup also reviews and approves requests to procure information technology not included on the Information Technology Standards List (see DOHP 50-9Information Technology Acquisition Policy).

Information User or **Information Resource User** -See End User

Insider Threat - An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Integrity - Safeguarding the accuracy and completeness of information and processing methods. The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Internet Email Access - The capability to access the department's email system by using an Internet web browser, which may or may not be on the state network.

Key - A means of access, control or possession. This may include electronic devices as well as manual locks.

Key Custodian - A DOH worker responsible for assisting information owners with access control and possession of information in designated secured areas.

Least Privilege - The security objective of granting users only those accesses they need to perform their official duties.

Local IT Disaster Recovery Coordinator - The person in the local office who has been assigned the responsibility for planning and directing the detailed information technology activities before, during, and after the disaster.

Malware - Malicious software, such as computer viruses, network worms, Trojan horses, logic bombs, and spy ware, for which special controls should be employed to prevent, detect and remove such software from department computers.

Media Sanitization - A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Members of the Workforce - Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the department, is under the direct control of the department, whether or not they are paid by the department. This includes members of other "State Agencies" who under *Florida Statute* provide services to the department, in particular members of the State Data Center systems Primary Data Centers.

Minimum Necessary Rule - Criteria designed to limit the request for Protected Health Information (PHI) to the information reasonably necessary to accomplish the purpose for which the request is made. This is an application of the concepts of "least privilege" and "need to know" to PHI.

Mobile Computing Device - A laptop, tablet, smartphone or other portable device that can

process data.

Mobile Devices - A general term describing both mobile computing 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, cell phones and tape drives that may be - attached to and detached from computing devices.

Multifactor Authentication - Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (e.g. password/PIN); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric).

National Institute of Standards and Technology (NIST) - NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Need to Know - A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.
Next of Kin - The spouse and children of a deceased individual. A spouse or child has equal authority to access patient medical records of a deceased person. If a personal representative is required to access records, then a next of kin is not adequate.

Notice of Privacy Practice - A federally mandated document with specific content requirements to be made available to individuals having protected health information maintained by the department in an activity under the jurisdiction of the federal HIPAA Privacy Rule. The specific requirements are detailed at 45 CFR 164.520.

Owner - See Information Owner

Patient Medical Information (PMI) - The unique set of information controlled by the interaction of the HIPAA Privacy Rule (45 CFR 160) and more stringent Florida laws such as Florida Healthcare practice and hospital laws, Sections 456.057 *F.S.*, 395.3025 *F.S.*, and other state healthcare confidentiality laws and rules.

Password - A protected word or string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

Password Management - A process or technology that allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor, and repair their own problem, without calling the help desk.

Patch - An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management - The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Personal Identifier or User Identification Code - A data item associated with a specific individual that represents the identity of that individual.

Protected Health Information - 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 as 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

Public Health Activities - Activities that are performed for the good of the community in the prevention, surveillance and control of disease by an agency that has the authority of the U.S. or state and that is responsible for public health matters as part of its official mandate.

Public Health Exemptions - Individually identifiable health information collected by the department for public heath purposes, but not for the provision of healthcare services to the individual is generally not subject to the federal Privacy Rule expressed in HIPAA, 45CFR160.103.

Individually identifiable health information collected by the department for purposes of statutorily authorized public health activities in the regulation of state controlled substances; reporting of disease, injury, child abuse, birth, or death; for public health surveillance, investigation, or intervention; and the monitoring of healthcare plans is specifically not subject to the federal Privacy Rule expressed in HIPAA, 45CFR160.203.

Particular state laws will control the confidentiality of collected individually identifiable health information for public health purposes when the HIPAA Privacy Rule is not applicable. Examples of confidential information exempt from HIPAA but still restricted from disclosure include information collected during public health disasters, bioterrorism events, communicable disease surveillance, epidemiologic investigations, syndromic surveillance, disease intervention investigations, environmental health investigations, disease screening activities, child abuse registries and reports made to the Department of Children and Families regarding missing children.

Confidential public health surveillance registries include Tuberculoses (TB), Sexually Transmitted Diseases (STD), Human Immunodeficiency Virus (HIV), Cancer/Tumor, Immunization, Vital Statistics, Brain and Spinal Cord Injuries, Infant Death, Trauma, Child Death Reviews and other communicable diseases reported to the Division of Disease Control as required by Chapter 64D-3, *F.A.C.* Information from these registries cannot be released except as outlined in the applicable *Florida Statutes* or *Florida Administrative Codes*.

Public Information - All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the 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 which is not confidential and has not been exempted from public disclosure by statute.

Recording Devices - A camera, an audio or video recorder, or any other devise to record, transfer sounds or images, or transmit a motion picture or any part of by means of any technology now known or later developed.

Remote Access - The ability to connect to a computer from a remote location and exchange information or remotely operate the system.

Risk - The likelihood or probability that a loss of information resource or breach of security will occur.

Risk Analysis - See Risk Assessment.

Risk Assessment - A process that systematically identifies valuable information system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first.

Risk Management - Decisions and subsequent actions designed to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Root Administrator - A person with unlimited access privileges who can perform any and all operations on a computer.

Secured Area - An area designated to ensure the security and privacy of information; protect confidentiality and data integrity, and provides appropriate access to information.

Security Incident or Breach - An event which results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or intentional.

Security token - (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network application or service.

Service Set Identifier (SSID) - A sequence of characters that uniquely names a wireless local area network.

Special Needs Shelter - A temporary emergency facility capable of providing care to residents whose medical condition is such that it exceeds the capabilities of the Red Cross Shelter but is not severe enough to require hospitalization.

Smart card - A plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.

Social networking - Sites that enable people to connect with others to form an online community. Typically members describe themselves in personal web page profiles and form interactive networks, linking them with other members based on common features of social networking sites.

Streaming media - Sound (audio) and/or pictures (video) that are transmitted on the Internet in a streaming or continuous fashion, using data packets.

Syndromic Surveillance - Data systems which monitor the health status of a community and help to identify health trends and disease outbreaks.

Third Party - Third party is anyone other than the healthcare provider organization, including its employees and agents, and the patient or authorized patient representative.

Triple Data Encryption Standard (Triple DES or **3DES)** - A block cipher, based on DES, that transforms each 64-bit plaintext block by applying a data encryption algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

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

User - See End User

Vulnerability - A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security.

Vulnerability Assessment - An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

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.

Forms

Acceptable Use and Confidentiality Agreement

Authorization for Non-Routine Disclosure of Patient Medical Information

Cooperative Agreement between the DOH and Colleges and Universities

Corrective Action Plan

Information Technology Security Exception Request

Initiation of Services and Instructions

Standard Third Party Networking Connection Agreement

Third Party Network Connection Request

Transmittal Letter Suggested Language

Incident Reporting Policy, Forms and Instructions – Contact the Office of the Inspector General by phone at (850) 245-4141, by email at Incident_IG@flhealth.gov, or refer to their website at http://dohiws.doh.state.fl.us/divisions/Insp_General/IncidentReports.htm

Acceptable Use and Confidentiality Agreement

SECTION A The Department of Health (Department) worker and the supervisor or designee must address each item and initial.

Security and Confidentiality Supportive Data

W S

☐ ☐ I have been advised of the location of and have access to the Florida Statutes and Administrative Rules.

☐ ☐ I have been advised of the location of and have access to the core Department of Health Policies, Protocols and Procedures and local operating procedures.

Position-Related Security and Confidentiality Responsibilities

I understand that the Department of Health is a unit of government and generally all its programs and related activities are referenced in Florida Statutes and Administrative Code Rules. I further understand that the listing of specific statutes and rules in this paragraph may not be comprehensive and at times those laws may be subject to amendment or repeal. Notwithstanding these facts, I understand that I am responsible for complying with the provisions of policy DOHP 50-10. I further understand that I have the opportunity and responsibility to inquire of my supervisor if there are statutes and rules which I do not understand.

☐ ☐ I have been given copies or been advised of the location of the following specific Florida Statutes and Administrative Rules that pertain to my position responsibilities:

_____
_____
_____
_____

☐ ☐ I have been given copies or been advised of the location of the following specific core DOH Policies, Protocols and Procedures that pertain to my position responsibilities:

_____
_____
_____
_____

☐ ☐ I have been given copies or been advised of the location of the following specific supplemental operating procedures that pertain to my position responsibilities:

_____
_____
_____
_____

☐ ☐ I have received instructions for maintaining the physical security and protection of confidential information, which are in place in my immediate work environment.

☐ ☐ I have been given access to the following sets of confidential information:

_____
_____
_____
_____

Penalties for Non Compliance

☐ ☐ I have been advised of the location of and have access to the DOH Employee Handbook and understand the disciplinary actions associated with a breach of confidentiality.

☐ ☐ I understand that a security violation may result in criminal prosecution and disciplinary action ranging from reprimand to dismissal.

Acceptable Use and Confidentiality Agreement

☐ ☐ I understand my professional responsibility and the procedures to report suspected or known security breaches.

The purpose of this Acceptable Use and Confidentiality Agreement is to emphasize that access to all confidential information regarding a member of the workforce or held in client health records is limited and governed by federal and state laws. Confidential information includes: the client's name, social security number, address, medical, social and financial data and services received. Data collection by interview, observation, or review of documents must be in a setting that protects the client's privacy. Information discussed by health team members must be held in strict confidence, must be limited to information related to the provision of care to the client, and must not be discussed outside the department.

_____	_____	_____
DOH Worker's Signature	**Date**	**Supervisor or Designee Signature**

Understanding of the Florida Computer Crimes Act, if applicable.

The Department of Health has authorized you to have access to sensitive data through the use of computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media).

Computer crimes are a violation of the department's disciplinary standards and in addition to departmental discipline, the commission of computer crimes may result in felony criminal charges. The *Florida Computer Crimes Act, Chapter 815, F.S.*, addresses the unauthorized modification, destruction, disclosure or taking of information resources.

I have read the above statements and by my signature acknowledge that I have read and been given a copy of, or been advised of the location of, the *Florida Computer Crimes Act, Chapter 815, F.S.* I understand that a security violation may result in criminal prosecution according to the provisions of *Chapter 815, F.S.*, and may also result in disciplinary action against me according to Department of Health policy.

The minimum information resource management requirements are:

- Personal passwords are not to be disclosed. There may be supplemental operating procedures that permit shared access to electronic mail for the purpose of ensuring day-to-day operations of the department.
- Information, both paper-based and electronic-based, is not to be obtained for my own or another person's personal use.
- Department of Health data, information, and technology resources shall be used for official state business, except as allowed by the department's policy, protocols, and procedures.
- Only approved software shall be installed on Department of Health computers (DOHP 50-10.2).
- Access to and use of the Internet and email from a Department of Health computer shall be limited to official state business, except as allowed by the department's policy, protocols, and procedures.
- Copyright law prohibits the unauthorized use or duplication of software.

_____	_____	_____
DOH Worker's Signature	**Date**	**Supervisor or Designee Signature**
_____	_____	_____
Print Name	**Date**	**Print Name**

W=Worker S=Supervisor

Attachment E

AUTHORIZATION TO DISCLOSE CONFIDENTIAL INFORMATION

INFORMATION MAY BE DISCLOSED BY:

Person/Facility: _____ Phone #: _____

Address: _____ Fax #: _____

INFORMATION MAY BE DISCLOSED TO:

Person/Facility: _____ Phone #: _____

Address: _____ Fax #: _____

Other method of communication: _____

I specifically authorize release of information relating to: (initial selection)

☐ General Medical Record(s), including STD and TB ☐ Progress Notes ☐ History and Physical Results

☐ Immunizations ☐ Family Planning ☐ Prenatal Records ☐ Consultations

☐ Diagnostic Test Reports (Specify Type of Test(s))_____

☐ Other: (Specify)_____

I specifically authorize release of information relating to: (initial selection)

☐ HIV test results for non-treatment purposes ☐ Substance Abuse Service Provider Client Records

☐ Psychiatric, Psychological or Psychotherapeutic notes ☐ Early Intervention ☐ WIC

PUROPSE OF DISCLOSURE:

☐ Continuity of Care ☐ Personal Use ☐ Other (Specify):_____

EXPIRATION DATE: This authorization will expire (insert date or event)_____. I understand that if I fail to specify an expiration date or event, this authorization will expire twelve (12) months from the date on which it was signed.

REDISCLOSURE: I understand that once the above information is disclosed, it may be redisclosed by the recipient and the information may not be protected by federal privacy laws or regulations.

CONDITIONING: I understand that completing this authorization form is voluntary. I realize that treatment will not be denied if I refuse to sign this form.

REVOCATION: I understand that I have the right to revoke this authorization any time. If I revoke this authorization, I understand that I must do so in writing and that I must present my revocation to the medical record department. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company, Medicaid and Medicare.

_____ _____

Client/Representative Signature Date

_____ _____

Printed Name Representative's Relationship to Client

_____ _____

Witness (optional) Date

Client Name: _____

ID#: _____

DOB: _____

Attachment E

AGREEMENT BETWEEN THE STATE OF FLORIDA, DEPARTMENT OF HEALTH,
(____*name of CHD or CMS*____)
AND
(_____name of School_____)
An institution providing health care professionals education

The purpose of this agreement is to guide and direct a working relationship between the

(_____*name of the school*_____), *an institution providing health care profession education and hereinafter referred to as SCHOOL, and the State of Florida, Department of Health.*

(_____*name of CHD or CMS clinic*_____), *hereinafter referred to as CLINIC, for the provision of learning opportunities for the health care profession students.*

RECITALS

The SCHOOL agrees:

1. To provide competent faculty for the planning implementation of instruction, teaching, guidance, supervision, and evaluation of health profession students.

2. To be responsible for the quality of care rendered to the patients while the student is assigned to the patient.

3. To work in accordance with all of the CLINIC procedures, policies, protocols, rules and regulations in making plans for observations and/or practices in health care at the CLINIC facilities.

4. To provide necessary books, periodicals and teaching materials for its education program.

5. To submit to the CLINIC a schedule indicating the number and names of students who will be participating and the name of the faculty member who will be supervising the students during their rotation.

6. To plan student assignments in consultation with a representative of the CLINIC.

7. To designate a contact person for evaluation and scheduling of student rotations and otherwise be a facilitator of communication between the parties.

8. To provide direct supervision of students whenever students are at the CLINIC or will provide indirect supervision for the students engaged in mutually agreeable practicum experience with a preceptor at the CLINIC.

9. To initiate and/or participate in group conferences as mutually agreed upon with a designee or the CLINIC for the purpose of discussing objectives of the learning experiences and the student performance in caring for patients.

10. To obtain and maintain throughout the term of this agreement, or any renewal thereof, professional liability insurance insuring the SCHOOL, its employees, and its students who will be

in training under this agreement with limits of liability coverage in the amount of not less than One Hundred Thousand Dollars ($100,000) per claimant and Two Hundred Thousand Dollars ($200,000) per occurrence. As evidence of such coverage, the SCHOOL shall furnish to the CLINIC a certificate of insurance or a certificate of self-insurance prior to commencing services under this agreement and annually thereafter. Failure of the SCHOOL to obtain and maintain such coverage shall be grounds for immediate termination of this agreement. This clause is not applicable to State of Florida agencies and subdivisions which have liability responsibilities specified in Florida Statute section 768.28 which states, **Waiver of sovereign immunity in tort action; recovery limits; limitation on attorney gees; statute of limitations; exclusions; indemnification; risk management programs.**

11. The SCHOOL shall assure the student will maintain confidentiality of all data, files, and client records related to the services provided pursuant to the agreement and shall comply with state and federal laws, including, but not limited to, Sections 384.29, 381.004, and 445.667, Florida Statutes. Procedures will be implemented by the SCHOOL to ensure the protection and confidentiality of all confidential matters the students observe. There procedures shall be consistent with the Department of Health Information Security Policies, Protocols, and Procedures, September 1997, as amended, which is acknowledged by the SCHOOL upon execution of this agreement. The SCHOOL ensures the student will adhere to any amendments to the CLINIC security requirements provided during the period of this agreement. The SCHOOL will ensure the student's compliance with any applicable professional standards of practice with respect to client confidentiality.

The CLINIC agrees:

1. To provide health care profession students accepted into this program access to planned supervised program of internship experience.

2. To provide designated staff members as internship supervisor for student.

3. To designate a contact person for evaluation and scheduling of student rotations and otherwise be a facilitator of communication between the parties.

4. To make available to the faculty and students of the SCHOOL the CLINIC facilities as agreed upon by both of the designated contact persons.

5. To retain overall responsibility for providing patient care to all patients in the areas where students are assigned.

6. To remove from the clinic/intern program any student not conducting themselves in accordance with the procedures, protocol, regulations, rules, or statutes governing the CLINIC. If this should become necessary, the CLINIC will attempt to give the SCHOOL five (5) days notice unless at the sole discretion of the Director/Administrator of the CLINIC, immediate removal is deemed necessary.

AGREEMENT BETWEEN THE STATE OF FLORIDA, DEPARTMENT OF HEALTH,
(____*name of CHD or CMS*____)
AND
(_____name of School_____)
An institution providing health care professionals education

7. To provide the physical facilities, equipment, supplies, and patients to supplement an educational program in accordance with the objective of providing clinical/intern experience to health care profession students. This agreement may be modified by mutual consent at any time or may be terminated by either party by submitting notice of such intent, in writing, at least thirty (30) days in advance. This agreement will be effective after review and signature by the CLINIC and the SCHOOL for a period of one (1) year from the date of the agreement and shall be automatically renewed for one-year consecutive terms unless either party requests changes of termination of this agreement.

   This agreement will be effective beginning: _____

   Approved:

   (_____name of school_____)

   By:_____Date:_____

   FLORIDA DEPARTMENT OF HEALTH,
   (____name of CHD or CMS clinic____)

   By:_____Date:_____

   Approved as to Form and Legality:_____ _____
   (enter DOH attorney's name) Date

Attachment E

Corrective Action Plan – Annual Risk Assessment| Department of Health [Office Name]

ID	Weakness	Anticipated Completion Date	ACTION STEPS / Implementation Plans	Implementation Tasks	Current Status / Update	Point of Contact	Risk Level	Comments
7.VI.D.1.o.	Data backups are not locked in a secured area.	06/30/2015	Locks are being installed on doors to secured areas	1. Purchase Order has been created to have locksmith put locks on doors 2. Doors will remain locked at all times when no one is in the secured area	No updates – June 2015	John Doe	High	EXAMPLE

NOTES:

To determine the risk level of the weakness addressed in this Corrective Action Plan, please use the following chart (FIPS Publication 199): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or any information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or any information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or any information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Low (Amplification)- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the function is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Medium (Amplification) – A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is

significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

High (Amplification) – A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a sever degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in sever or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Mission:
To protect, promote & improve the health of all people in Florida through integrated state, county & community efforts.

Rick Scott
Governor

John H. Armstrong, MD, FACS
State Surgeon General & Secretary

Vision: To be the **Healthiest State** in the Nation

Department of Health
Office of Information Technology
Information Technology Security Exception Request
Information Security Manager (ISM)
DOHP 50-10 Policy Exception

Official Request From:

Program Office:

DOHP 50-10 Policy Chapter #:

Business Case and Justification:

Program Office Director/Administrator:

DOH Information Security Manager: Shon Bynum, Information Security Manager

DOH Chief Information Officer: Tony Powell, Chief Information Officer

---

☐ **APPROVED** ☐ **NOT APPROVED**

_____ _____
ISM Signature Date

Please return the completed form by email to: SecurityAdministration@flhealth.gov

Florida Department of Health
Office of Information Technology
4052 Bald Cypress Way, Bin B-05 • Tallahassee, FL 32399-1733
PHONE: 850/245-4256 • FAX 850/921-5149

www.FloridaHealth.gov
TWITTER:HealthyFLA
FACEBOOK:FLDepartmentofHealth
YOUTUBE: fldoh
FLICKR: HealthyFla
PINTEREST: HealthyFla

INITIATION OF SERVICES

PART I CLIENT-PROVIDER RELATIONSHIP CONSENT

Client Name: _____

Name of Agency: _____

Agency Address: _____

I consent to entering into a client-provider relationship. I authorize Department of Health staff and their representatives to render routine health care. I understand routine health care is confidential and voluntary and may involve medical office visits including obtaining medical history, examination, administration of medication, laboratory tests and/or minor procedures. I may discontinue the relationship at any time.

PART II DISCLOSURE OF INFORMATION CONSENT (treatment, payment or healthcare operations purposes only)
I consent to the use and disclosure of my medical information; including medical, dental, HIV/AIDS, STD, TB, substance abuse prevention, psychiatric/psychological, and case management; for treatment, payment and health care operations.

PART III MEDICARE PATIENT CERTIFICATION, AUTHORIZATION TO RELEASE, AND PAYMENT REQUEST (Only applies to Medicare Clients)

As Client/Representative signed below, I certify that the information given by me in applying for payment under Title XVIII of the Social Security Act is correct. I authorize the above agency to release my medical information to the Social Security Administration or its intermediaries/carriers for this or a related Medicare claim. I request that payment of authorized benefits be made on my behalf. I assign the benefits payable for physician's services to the above named agency and authorize it to submit a claim to Medicare for payment.

PART IV ASSIGNMENT OF BENEFITS (Only applies to Third Party Payers)

As Client/Representative signed below, I assign to the above named agency all benefits provided under any health care plan or medical expense policy. The amount of such benefits shall not exceed the medical charges set forth by the approved fee schedule. All payments under this paragraph are to be made to above agency. I am personally responsible for charges not covered by this assignment.

PART V MY SIGNATURE BELOW VERIFIES THE ABOVE INFORMATION AND RECEIPT OF THE NOTICE OF PRIVACY PRACTICES

_____ _____ _____
Client/Representative Signature | Self or Representative's Relationship to Client | Date

_____ _____
Witness (optional) | Date

PART VI WITHDRAWAL OF CONSENT

I, _____ WITHDRAW THIS CONSENT, effective _____
Client/Representative Signature | Date

_____ _____
Witness (optional) | Date

Client Name: _____
ID#: _____
DOB: _____

INITIATION OF SERVICES
Instructions

PART I - Acquires general consent to provide healthcare.

Client's Name: The client's name is printed or written on this line.

Name of Agency: The name of the agency where care is provided. It should be the CHD or CMS Region, not the specific location. Ex.: Orange County Health Department, not South Street Health Center.

Agency Address: The official address of the County Health Department of CMS Clinic, not the street address of the specific health center or program office.

PART II - Obtains authority required under state law to use patient medical information for payment and healthcare operations as well as treatment.

PART III - Acquires authority to bill Medicaid.

PART IV - Acquires authority to bill third parties such as insurance companies.

PART V

Client/Representative Signature: Client or client's representative signs form

Self or Representative's Relationship: Enter the work "self" if the client signs the form. If the form is signed by the representative then the representative enters their relationship to the client (must have legal authority to sign for patient). Ex.: parent, guardian, foster parent

Date: Date form is signed

Witness: Signature of employee, if any, who witnessed the signature of the client or representative.

Date: Date form signed and witness signed

PART VI

The client or representative writes their name in the space, following "I" and enter the effective date the withdrawal becomes effective. The person requesting the revocation of consent signs the form, completes relationship as described above and dates the form. The Witness signs and dates the form they observed being signed.

Client Identification

The label with client identification is placed in this location or the client's name and identification is entered here by hand or computer.

Attachment E

STATE OF FLORIDA

DEPARTMENT OF HEALTH

STANDARD THIRD PARTY NETWORKING CONNECTION AGREEMENT

THIS AGREEMENT is entered into between the State of Florida, Department of Health, hereinafter referred to as the *Department*, and

_____, hereinafter referred to as the *user*.

THE PARTIES AGREE:

I. THE USER AGREES:

A. Usage of Network Connection Services

That all use of the network connection services by user's employees or agents shall be limited to the approved services and business activities only. User agrees that each employee or agent (currently or in the future) using the Department network reads the Department's computer use and information security policies and procedures and signs a usage statement attesting compliance with those policies. Signed usage statements will be delivered to the Department's representative prior to an individual using the system. User agrees to notify the Department in writing within twenty-four (24) hours of employee resignations or layoffs, and immediately for involuntary terminations.

B. Cost of Network Connection

To pay all costs to install, maintain, and disconnect the requested network connection.

C. DOH-Owned Equipment

To properly use, maintain, secure and return (at agreement termination or other request of the Department) the Department-owned equipment listed below (attach additional sheets if necessary):

ITEM	SERIAL NUMBER	ASSET TAG NUMBER	USER LOCATION

D. To the Following Governing Law

1. State of Florida
   This agreement is executed and entered into in the state of Florida, and shall be construed, performed and enforced in all respects in accordance with the laws, rules, and regulations of the state of Florida. Each party shall perform its obligations herein in accordance with the terms and conditions of the agreement.
2. Federal Law
   HIPAA: Where applicable, the user will comply with the Health Insurance Portability and Accountability Act as well as all regulations promulgated thereunder (45CFR Parts 160, 162, and 164) .

E. Venue

Any legal action pertaining to this contract shall be maintained in the Circuit Court, Second District, Leon County, Florida.

F. Audits, Records and Records Retention

1. To retain all records pertinent to this agreement for a period of six (6) years after termination of the agreement, or if an audit has been initiated and audit findings have not been resolved at the end of six (6) years, the records shall be retained until resolution of the audit findings or any litigation which may be based on the terms of this agreement.
2. To assure that these records shall be subject at all reasonable times to inspection, review, or audit by federal, state, or other personnel duty authorized to the department.

NOTE: Paragraphs I.F.1. and I.F.2. are not applicable to agreements executed between state agencies or subdivisions, as defined in §766.28, Florida Statutes.

G. Monitoring by the Department

To permit persons duly authorized by the Department to inspect any records, papers, documents, facilities, goods and services of the user, which are relevant to this agreement, conduct site visits, and interview any clients and employees of the user to assure the Department of satisfactory performance of the terms and conditions of this agreement. The user's failure to correct noted deficiencies may, at the sole and exclusive discretion of the Department result in the user being deemed in breach or default of this agreement and the termination of this agreement for cause.

H. Indemnification

1. The user shall be liable for and shall indemnify, defend, and hold harmless the Department and all of its officers, agents, and employees from all claims, suits, judgements, or damages, consequential or otherwise and including attorneys' fees and costs, arising out of any act, actions, neglect, or whether direct or indirect, and whether to any person or tangible or intangible property.
2. The user's inability to evaluate liability or its evaluation of liability shall not excuse the user's duty to defend and indemnify within seven (7) days after such notice by the Department is given by certified mail. Only adjudication or judgement after highest appeal is exhausted specifically finding the user not liable shall excuse performance of this provision. The user shall pay all costs and fees related to this obligation and its enforcement by the Department. The Department's failure to notify the user of a claim shall not release the user of the above duty to defend.

I. Assignments and Subcontracts

1. To neither assign the responsibility of this agreement to another party nor subcontract for any of the work contemplated under this agreement without prior written approval of the Department, which shall not be unreasonably withheld. Any sub-license, assignment, or transfer otherwise occurring shall be null and void.
2. This agreement will become null and void upon sale, acquisition, or merger of the user. Upon such event, any network services shall be discontinued and at the department's discretion, renegotiated wit the new entity.
3. The state of Florida shall at all times be entitled to assign or transfer its rights, duties, or obligations under this agreement to another governmental agency in the state of Florida, upon giving prior written notice to the user. In the event the state of Florida approves transfer of the user's obligations, the user remains responsible for all work performed and all expenses incurred in connection with the agreement. In addition, this agreement shall bind the successors, assigns, and legal representatives of the user and of any legal entity that succeeds to the obligations of the state of Florida.

J. Information Security

The user shall maintain confidentiality of all data, files, and records including client records related to the services pursuant to this agreement and shall comply with state and federal laws, including, but not limited to §384.29, 381.004, 392.65, and 456.057, F.S. Procedures must be implemented by the user to ensure the protection and confidentiality of all confidential matters. These procedures shall be consistent and in compliance with the Department of Health Information Security and Computer Use Policies, which is incorporated herein by reference, and the receipt of which is acknowledge by the user, upon execution of this agreement. The user must also comply with any applicable professional standards of practice with respect to client confidentiality. The user will immediately notify the Department Information Security Manager (ISM) contact of any violations of Department of Health Information Security and Computer Use Policies.

II. THE DEPARTMENT AGREES:

A. Network Connection Service

To provide the following network connection services to the user: _____
_____
_____
_____
_____
_____
Cost arrangements for the user will be as follows:_____

III. THE USER AND THE DEPARTMENT MUTUALLY AGREE:

A. Effective and Ending Dates

This agreement shall begin on _____ or on the date on which the agreement has been signed with both parties, whichever is later. This agreement shall end on _____.

B. Termination

1. Termination at Will

This agreement may be terminated by either party upon no less than thirty (30) calendar days notice in writing to the other party, without cause, unless a lesser time is mutually agreed upon in writing by both parties. Said notice shall be delivered by certified mail, return receipt requested, or in person with proof of delivery.

2. Termination for Cause

This agreement may be terminated and the network connection immediately terminated, at the state's discretion, if any violation of Department of Health Information Security and Computer Use Policies is detected. The provisions herein do not limit the Department's right to remedies at law or in equity.

STANDARD THIRD PARTY NETWORKING CONNECTION AGREEMENT

C. Representatives (Names, Addresses, Telephone Numbers, and Email Addresses)

Primary Contact:
Name: _____
Address: _____
City/State/Zip: _____
Phone Number: _____
Email Address: _____

Technical Contact:
Name: _____
Address: _____
City/State/Zip: _____
Phone Number: _____
Email Address: _____

Organization Where Network Connection will Terminated:
Name: _____
Address: _____
City/State/Zip: _____
Room Number: _____
Email Address: _____

Department of Health Security Contact:
Name: _____
Address: _____
City/State/Zip: _____
Phone Number: _____
Email Address: _____

Upon change of representatives (names, addresses, telephone numbers) by user, notice shall be provided in writing to the Department within twenty-four (24) hours of such change, and said notification attached to originals of this agreement.

D. Background Checks Required? Yes☐ No☐

E. All Terms and Conditions Included or Addendum to Existing Agreement (Check which applies).

_____This agreement and its attachments as referenced, _____ contain all the terms and conditions agreed upon by the parties. There are no provisions, terms, conditions, or obligations other than those contained herein, and this agreement shall superseded all previous communications, representations, or agreements, either verbal or in written between the parties. If any term or provision of the agreement is found to be illegal or unenforceable, the remainder of the agreement shall remain in full force and effect and such term or provision shall be stricken.

_____This agreement and its attachments are an addendum to contract #_____.
The terms and conditions contained herein and the original contract constitute the entire agreement. The terms and conditions in this document shall supersede any conflicting language in the original contract. If any term or provision of the original contract or this document is found to be illegal or unenforceable, the remainder of the contract shall remain in full force and effect and such term or provision shall be stricken.

I have read the above agreement and understand each section and paragraph.
IN WITNESS THEREOF, the parties hereto have caused this page agreement to be executed by their undersigned officials as duly authorized.

USER
SIGNATURE: _____
NAME: _____
TITLE: _____
DATE: _____
STATE AGENCY 29-DIGIT FLAIR CODE:_____
FEDERAL EID# (OR SSN): _____
USER FISCAL YEAR ENDING DATE: _____

STATE OF FLORIDA, DEPARTMENT OF HEALTH – OFFICE OF IT
SIGNATURE: _____
NAME: _____
TITLE: _____
DATE: _____

THIRD PARTY
NETWORK CONNECTION REQUEST

All requests for Third Party Network Connections must be accompanied by this completed Network Connection Request. Please attach additional sheets, if necessary. Background checks may be required, depending upon the information and systems to be accessed.

DOH Sponsoring Office/Unit: _____

External entity requesting network connection: _____

Requestor:
Name: _____
Address: _____
Entity Head's Name: _____
Phone Number: _____ Mobile Number: _____
Email Address: _____

Technical Contact:
Name: _____
Phone Number: _____ Mobile Number: _____
Email Address: _____

Alternate Technical Contact:
Name: _____
Phone Number: _____ Mobile Number: _____
Email Address: _____

Purpose of Connection Request:
Please describe the needs of the proposed connection. Please include information about the type of work done over the Network Connection, the applications to be used, the type of data transfers done, the number of files involved, and the estimated hours and times of use each week, the privacy requirements (if encryption is needed), bandwidth needs, and if a secondary connection is needed.

_____
_____
_____
_____
_____
_____

Does the request involve research? Y ☐ N ☐ *Research requests must be reviewed by the Department's Human Subjects Research Board and should be referred to the Director of Statewide Research*

What is the requested installation date (Minimum lead-time is 60 days): _____

What is the approximate duration of the Third Party Network Connection: _____
Location (address) of termination point (demark) of the Network Connection (including building number, floor, and room number) and instructions for location of the connection in that room:

_____
_____
_____
_____
_____

Please list any existing network connections of the entity to the Florida Department of Health:

THIRD PARTY
NETWORK CONNECTION REQUEST

Is the network connection required as part of another contract with the Department? If so, please identify the department contact and contract, including contract number if assigned:

Has a Non-Disclosure Agreement been signed with the appropriate employees of the Third Party? ___
Please attach copies for each user and list below. Attach a separate sheet if necessary.

Employee Name	Employee Phone Number	Employee Email Address

Second External Entity Information (if another organization or party is involved, please explain relationship to requestor and details regarding their use of this connection:

Entity Name: _____
Entity Head/Requestor Name: _____
Technical Contact: _____
Phone Number: _____ Mobile Number: _____
Email Address: _____

Location (address) of termination point (demark) of the Network Connection (including building number, floor, and room number) and instructions for location of the connection in that room:

Has a Non-Disclosure Agreement been signed with the appropriate employees of the Third Party? ___
Please attach copies for each user and list below. Attach a separate sheet if necessary.

Employee Name	Employee Phone Number	Employee Email Address

Other useful information:

Attachment E

Transmittal Letter
Suggested Language

☐ If the purpose of the information supplied in this transmittal is for healthcare treatment, all patient medical information is supplied, excluding: substance abuse service provider client records; psychiatric, psychological or psychotherapeutic notes; early intervention, or WIC data unless a specific authorization or court order was supplied.

☐ If the purpose of the information supplied in this transmittal is for healthcare operations or payment, the minimum necessary patient medical information is supplied, excluding: HIV test results; substance abuse service provider client records; psychiatric, psychological or psychotherapeutic notes; early intervention, or WIC data unless a specific authorization or court order was supplied.

☐ If the purpose of the information supplied in this transmittal is for a purpose other than the above two, the patient medical information as described in the authorization to disclose, the applicable subpoena, or in the court order for disclosure is supplied, excluding: HIV test results; substance abuse service provider client records; psychiatric, psychological or psychotherapeutic notes; early intervention, or WIC data unless a specific authorization or court order was supplied.

SUMMARY OF CONFIDENTIALITY STATUTES
SHIELDING DOCUMENTS IN THE CUSTODY OF THE DEPARTMENT OF HEALTH
(Updated June 2015)

The following statutes shield documents from disclosure as a public record. Depending on the specific statute; a court order, subpoena, or release is required for disclosure. The most comprehensive resource on public records and public meetings is the **GOVERNMENT-IN-THE-SUNSHINE MANUAL** published by the "First Amendment Foundation" and reviewed annually by the Attorney General's Office.

39.0132	Proceedings relating to children-records and information
39.201(1)(b)	Names of child abuse reporters
39.202	Child abuse reports and records
63.162, 63.165	Adoption proceedings – registry
63.165(1)	Registry of adoption information
110.1091	Employee participation in "employee assistance program"
110.201(4)	Collective bargaining
112.0455(8)(l) & (u), (11)	Drug-Free Workplace Act, Employee – drug screening
112.21(1)	Employee participants in tax sheltered annuities
112.215(7)	Employee participants in deferred compensation programs
112.3188	Disclosure to Inspector General or Internal Auditor
119.07(3)	Exemptions from public record disclosure
121.031(5)	State retirees – names and addresses
163.64	Multi-agency collaborative information system, sharing OK
215.322(6)	Credit card numbers
281.301	Security of state property – records & meetings
282.318	Security of state information technology resources
365.171(15)	"911" recordings
381.0031(4)	Disease Reports – exception, may be made public "only when necessary to protect public health"
381.004(3)	HIV testing & results
381.0055	Shared information retains confidential status
381.0056(5)(p), 1002.22	Individual student health services records
381.775	Brain & Spinal Cord Injury – applicant or recipient
381.83	Trade secrets
381.95, 395.1056	Terrorism – features and capabilities of regulated medical facilities
382.008(6)	Death certificates – family & personal information
382.013(5)	Birth certificates – family & personal information
382.015	New birth certificate – sealing of original
382.025	Birth records; other vital records
383.14(3)(d)	Registry – pre and post-natal screening
383.32(3)	"Birth Center" clinical records

383.402	Certain records received or created by State Child Abuse Death Review Committee or local child abuse death review committee
383.51	Parent leaving newborn at hospital or fire dept
384.26	STDs – contact investigations
384.282	Judicial proceeding for STD examination
384.287	Screening for STDs for certain professions after a significant exposure
384.29	STD confidentiality provisions
384.30	STDs – examination and treatment of minor
385.202	Cancer registry – identifying information
392.54	Tuberculosis – contact investigation
392.545	Judicial proceeding for tuberculosis examination
392.65	Tuberculosis confidentiality provisions
394.907(7),395.0193(7), 397.419(7)	Discipline file, quality assurance, peer review
395.0197(6),8)&(14)	Hospital internal risk management
395.1056	Hospital Emergency Plans – terrorism
395.3025(4)(e)	Hospital – patient records, exceptions for discipline, abuse investigations and other purposes
395.3035	Public hospital – records and meetings
395.4025(9) & (12)	Trauma Center – registry & other records
395.404	Trauma registry data
395.50 & .51	Local trauma agency – quality assurance
401.30(3)&(4)(g)	EMS records
401.414	EMS discipline
401.425	EMS quality assurance
405.03	Medical information for research
406.135	Autopsy photos, videos, audios
408.061(11)	AHCA, exempt records from
409.821	Florida Kidcare application
413.341(1)	Vocational Rehabilitation (now at DOE)
415.107	Vulnerable adults – abuse, neglect, & exploitation
435.09	Confidentiality of personnel background check information
443.1715	Reemployment Assistance – identity of applicant
447.605	Collective bargaining – Secretary and Legislature
456.013(12)	Social security numbers of licensees; limited disclosure in Title IV-D program for child support enforcement
456.014(1)&(2)	Information required of an applicant– exceptions
456.017(4)	Meetings to develop examination questions – any public records generated confidential
456.043	Practitioner profile, access to AHCA confidential records; data storage
456.046	Practitioner profile, patient names and other identifying information
456.051(1)	Name of injured person or claimant on reports of professional liability

456.057(8)(a)	Patient records – and other documents identifying patients by name
456.061	Disclosure of HIV information under certain circumstances
456.073(2)	Complaint dismissed prior to probable cause
456.073(10)	Complaint until 10 days after probable cause
456.076(3)(e)&(5)(a)	Impaired practitioner
456.078(4)	Mediation of complaint
456.081	Publication of information
456.082	Disclosure of confidential information
458.337(3), 459.016(3)	Discipline by peers or organization, report to DOH, report inadmissible in admin or judicial proceeding
458.339(3)	Discipline, implied consent to report on mental or physical health of licensee
458.341	Search warrant, patient records require patient consent
459.017(2) & (3)	Discipline, osteopath, implied consent health report
459.018	Search warrant, osteopath
464.208	Certified Nursing Assistants – background screening info obtained from ACHA
465.017(2)	Pharmacy-except for DOH, subpoena (notice to patient)required for Rx
466.022(3)	Dental – Peer review useable only as background
466.0275	Dentist, discipline, implied consent to health report
466.041(3)	Dental – hepatitis B status
487.041(7)	Pesticide registration
499.012(3)(g) & (m)3.	Drug wholesaler permit application info
499.051(7)	Complaint and investigative info re Drug, Device & Cosmetic Act, also trade secret
624.91(7)	Fla. Healthy Kids Corp.- medical & financial ID
741.04	Social Security numbers on marriage license application
760.11(12)	Commission on Human Relations – complaint
766.101(7)(c)	Report of medical review committee, useable only as background in discipline
766.106(7)(c)	Malpractice, medical examination of claimant
766.1115(4)(c)	Sovereign immunity, adverse incident reports
768.28(15)(b)	Risk management- claims file, minutes
828.30(5)	Rabies vaccination certificate
945.6032(3)	Correctional Medical Authority – review committee
951.27(2)	Disclosure to victim – inmate blood test results
960.003	Victim of HIV infected assailant
1002.22	Educational records – school health records – student right to privacy
1004.445(9)	Florida Alzheimer's Center and Research Institute – personal identifying information, medical records, trade secrets and related information, donor information

SUMMARY OF DOH CONFIDENTIALTY RULES

64C-7.006	Metabolic and Heredity Disorder Screening Records
64C-7.010	Infant risk screening records (prenatal & postnatal)
64D-2.003	HIV
64D-2.004	HIV
64D-2.006	HIV
64D-3.016 & 3.017	STD reports including HIV and AIDS
64D-3.018	Partner notification
64F-6.005	School health records – students
64F-7.004	Family planning–notification of abnormal lab results
64F-10.008	Primary care projects – client records
64F-12.021	Fla. Drug Device & Cosmetic Act – trade secrets

I. Virus Proliferation. The primary ways in which viruses propagate to other devices include:

A. Sharing infected mobile storage devices between users.

B. Downloading programs from the internet.

C. E-mail attachments.

II. **Virus Symptoms -** There are various symptoms of viruses that may be experienced when using an infected computer or device. The main indications include:

A. Unexpected changes in file sizes and contents.

B. Unexplained appearance of unknown files.

C. Reassignment of system resources.

D. The unaccounted use of Random Access Memory (RAM) or a reduction in the amount known to be in the machine.

E. Abnormal CPU utilization. An indicator of high CPU use is a constantly running fan, which is used to cool the CPU during operations.

F. Unusual 'pop-up' windows on your desktop.

III. Virus Prevention - Preventing a virus from infecting Department of Health information technology resources requires virus awareness among all users. The basic anti-virus practices and techniques described below are to be employed by all members of the workforce in order to minimize the risk of introducing viruses and other malicious software, to ensure timely detection of virus infections, to eliminate virus infections from the inventory of computers, and to minimize the risk of malicious programs propogating to other systems.

A. Check all new software for infections before installing it. It is advisable to use multiple anti-virus programs to scan the software, when available. No single anti-virus software is able to detect all viruses.

B. Do not install any software on a workstation unless the software has been approved for use and scanned for viruses.

C. Do not download software from internet without prior approval.

D. Do not use external storage devices from home systems or other external sources that have not been scanned for viruses. Only Departmen authorized external devices may be used on DOH workstations and servers unless authorized by the Information Security Manager or delegate.

E. Protect system files, critical data files, and applications by making back up copies and storing them on the network or write-protected external drives.

F. A system administrator should have a back up copy of every software program each time it is modified in accordance with established software development procedures and controls.

IV. Virus Response - If a computer is believed to be infected with a virus, the following steps should be followed:

A. Stop; do not turn off the workstation.

B. Remove infected machine from the network.

C. Identify, in writing, what activity indicated a virus may be present.

D. Contact your supervisor, security coordinator or system administrator, immediately.

E. Report all suspicious activity to your supervisor and the security coordinator. Only a rapid response will result in the successful containment and removal of a virus. Once a virus infection has been determined, the need exists to eradicate the virus, prevent its spread and re-infection, and bring the newly cleaned system back into full production.

F. Users must not attempt to eradicate a computer virus from their system unless they do so while in communication with a systems administrator. This communication will help minimize damage to data files and software, as well as ensuring that information needed to detect a re-infection has been documented.

G. The security coordinator will respond to incidents of suspected viruses and initiate the OIG Incident Reporting Process, as necessary. They will verify that there is a virus and work with appropriate personnel, usually the system administrator, to clean the workstation using the following virus response procedures:

1. Boot the workstation from write-protected removable media containing the anti-virus software, such as a flash drive or optical disc (CD/DVD).

2. Scan the hard drive (memory, boot sector, and all files) for viruses.

3. Identify and document by name any viruses found.

4. Clean any specific viruses found.

5. Rescan the hard drive.

6. Scan and clean all removable media.

7. Attempt to determine source of infection for tracking purposes.

8. Determine any other infections that may have occurred as a result of the original infection.

9. Report results to management.

10. Restore any lost software from its original write-protected media.

H. Attempt to restore from known-good backups any data that may have been lost or altered.

I. Log type of virus and measures taken to eradicate virus. Logs are to be reported to the Security Administration Team on the last Friday of each month.

I. Poor and/or weak passwords have the following characteristics:

A. The password contains fewer than eight characters.

B. The password is word found in a dictionary.

C. The password is common usage word such as:

1. Names of family, pets, friends, co-workers, fantasy characters, etc.
2. Computer terms and names, commands, sites, companies, hardware, software.
3. Birthday and other personal information such as addresses and phone numbers.
4. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
5. Any of the above spelled backwards.
6. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

II. Good passwords have the following characteristics:

A. Contain both upper lower case characters (e.g., a-z, A-Z).

B. Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+{}|)

C. Are eight or more alphanumeric characters.

D. Are not words in any language, slang, dialect, jargon, etc.

E. Are not based on personal information, names of family, etc.

III. Pass-phrase

A. A pass-phrase may take the place of a password during authentication to the DOH network.

B. The pass-phrase is a sequence of characters that is longer than a password. For example, “DiamondsReallyAreYourbestfriend”?

C. The user generates the pass-phrase just like when a user creates a password.

D. A pass-phrase is more secure than a password because it is longer and harder to obtain by an attacker.

I. Homeland Security and Patriot Acts

Congress passed the Homeland Security Act and the Patriot Act in order to protect the citizens of the United States from any potential or viable threat. The U.S. government is permitted to access any and all information it deems necessary to protect the nation. The challenge of these laws is to decide whether the gap between national security and personal privacy is small or large and how the security of the nation can be maintained and still protect the privacy of the patient. Public health information systems provide important information for national security efforts without compromising patient privacy.

A. Homeland Security Act

The Homeland Security Act's three primary purposes are (1) to prevent terrorist attacks within the U.S., (2) reduce the vulnerability of the U.S. to terrorism, and (3) to minimize damage and assist in recovery of terrorist attacks. The Secretary of Homeland Security has the authority to direct and control investigations that require access to information needed to investigate and prevent terrorist attacks. This would include protected health information (PHI) of any type without the authorization of the patient or legal guardian. The Homeland Security limits the use of PHI for use only in the performance of official duties and disclosure is limited to those with a specified "need to know" related to the investigation. This act is seen as compatible with HIPAA.

B. Patriot Act

The purpose of the Patriot Act is to deter and punish terrorist acts within the U.S. and around the world and to enhance law enforcement investigations. The Patriot Act permits emergency disclosure of electronic communications to protect life. The director of the FBI or his designee may apply for an order requiring the production of any tangible things; which would include PHI, for an investigation to protect against terrorism nationally or internationally. The Patriot Act has specific procedures that must be followed when PHI is required under the Patriot Act. An application for production must be made to a judge or magistrate, and the judge must demonstrate that the records requested are needed for an authorized investigation.

The act states, "A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production, such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context."

II. Disclosure of Public Health Information (PHI)

When PHI is requested, the appropriate identity of the government official, the office location and government branch of the requestor should be obtained. The health information professional should know that the requestor has the authority by law to receive the PHI. The disclosure of the PHI should be documented in the accounting of disclosures. A parent or legal guardian's signature is not required when a request is

made under the authority of the Homeland Security and Patriot Acts. The Patriot Act requires an Order of Production signed by a judge.

III. Syndromic Surveillance Systems

Syndromic surveillance systems are to monitor non-specific clinical information that may indicate a bio-terrorism associated disease before the actual diagnosis can be made. Usually the health information used in syndromic surveillance systems is de-identified when transmitted to the public health authority. The collection of health data is to identify clusters of cases, rather than individual cases.

IV. Vital Statistics Data

The basic reason for confidentiality of vital records is a person's right to privacy. Vital records involve the most intimate affairs of an individual. Hospitals and physicians are mandated by law to provide the information for vital records. They provide this information with the understanding that the privacy will not be abused.

Information contained in the vital records data is received from any sources which may include parents, spouse, family members, physicians, hospital/medical records, and other persons that may have knowledge of pertinent facts such as funeral directors.

Birth records are available only to persons specified by statute. The registrar has the responsibility to ensure access to birth records must meet the requirements specified in statute. Birth records over 100 years old do not have the same confidentiality restrictions.

Death records do not have the same level of confidentiality as birth records. Death records contain the physician's statement as to the cause and circumstances of the death and are a legal extension of the doctor patient relationship. The cause of death section is confidential and available only to persons identified in statute. Death records with the cause of death section may be released if the record is over 50 years old.

Access to confidential vital records can be granted by DOH for the purposes of health planning, evaluation and research.

V. Certified copies of birth certificates may be obtained only by the person identified on the birth record, if of legal age; parent or guardian or legal representative. One hundred years after the date of birth, the birth record becomes public information and can be issued to any applicant. Some records of births that occurred in Florida may be available as far back as 1865.

VI. Certified copies of death certificates with the cause of death may be obtained by the registrant's spouse or parent, child, grandchild or sibling, if of legal age and to any person providing a will, insurance policy or other document demonstrating their interest in the estate of the decedent. Anyone may obtain a copy of the certificate without the cause of death section. After 50 years from the date of death, cause of death information is no longer exempt from Section119.07 *F.S.* Some records for deaths in Florida may be found as far back as 1877.

VII. Certified copies of the original marriage certificate may be obtained for marriages taking place in Florida after June 6, 1927. Information on marriages prior to that date must be obtained from the court issuing the license.

VIII. Certified copies of divorce notice may be obtained if the divorce took place after June 6, 1927. The names of both husband and wife must be provided in order to locate the divorce information. Information on divorces occurring before June 6, 1927, must also be obtained from the court that granted the decree.

IX. Protection of Vital Record Forms: The original birth certificate paper is numbered and recorded. These blank forms must be secured and protected at all times. These forms can be used for illegal and bogus criminal activities.

The original death certificate paper is numbered and recorded. These blank forms must be secured and protected at all times. These forms can be used for illegal activities but do not have the high demand that the birth certificate forms do.

X. **School Health Records:** The Family Education Rights and Privacy Act (FERPA) is a federal law that protects student education records. Student health records maintained at the school by the school are considered student education records as defined by FERPA. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when the student reaches the age of majority (18). Parents must authorize the disclosure of information from the records; however, FERPA identifies specific conditions when the information may be disclosed without the parental authorization. Refer to 20 U.S.C. 1232g, 34 CFR Part 99, and Section 318.0056, *F.S.*

XI. **Environmental Health Records:** Records created and maintained by the Environmental Health Division are public records with the exception of food borne illness records which are treated as confidential medical records.

When these records are requested, the request is usually for more than one client. All or many of the clients involved in the food borne illness event may be requested. In this case, patient identifiers other than the requestor should be redacted prior to release.

XII. **Child Care Facility Records:** These records are public records with the exception of records that identify abuse or personal health information which would identify an individual. Redaction of all personal identifiers should be completed prior to release of information.

XIII. **Epidemiology Records:** Since most of the records related to an epidemiology event contain medical information and individual identifiers, these records are treated as confidential medical records.