

The Florida Department of Health

Information Security and Privacy Policy

Copyright © 2005, 2007, 2008 by the Florida Department of Health. All rights reserved. The entire contents of this publication are the property of the Florida Department of Health. User may not copy, reproduce, distribute display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, without the express written consent of the Florida Department of Health. Without limiting the foregoing, user may not reproduce, distribute, re-publish, display, modify, or create derivative works based upon all or any portion of this publication for purposes of teaching any computer or electronic security courses to any third party without the express written consent of the Florida Department of Health.

**DEPARTMENT OF HEALTH INFORMATION SECURITY AND PRIVACY POLICY
TABLE OF CONTENTS
DOHP 50-10-07**

DOHP 50-10-07	Security 1 – Information Security and Privacy	5									
DOHP 50-10a-07	Security 2 – Data Classification	8									
DOHP 50-10b-07	Security 3 – Designation of Key Security and Privacy Personnel	11									
DOHP 50-10c-07	Security 4 – Acceptable Use and Confidentiality Agreement	20									
DOHP 50-10d-07	Security 5 – Security and Privacy Awareness Training	29									
DOHP 50-10e-07	Security 6 – Secured Areas and Physical Security Procedures	32									
DOHP 50-10f-07	Security 7 – Confidential Information	36									
DOHP 50-10g-07	Security 8 – Disclosure of Confidential Information	42									
DOHP 50-10h-07	Security 9 – Patient Privacy Rights	52									
DOHP 50-10i-07	Security 10 – Public Health HIPAA Exemptions	58									
DOHP 50-10j-07	Security 11 – Contract Providers and Business Associates	61									
DOHP 50-10k-07	Security 12 – Retention, Archiving, and Disposition of Records	65									
DOHP 50-10l-07	Security 13 – Risk Analysis	69									
DOHP 50-10m-07	Security 14 – Contingency Planning	72									
DOHP 50-10n-07	Security 15 – Information Resource Management Security	78									
Appendix A	Definitions and Glossary	88									
Appendix B	Forms <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Acceptable Use and Confidentiality Agreement</td> </tr> <tr> <td style="padding: 2px;">Authorization for Non-Routine Disclosure of Protected Health Information</td> </tr> <tr> <td style="padding: 2px;">Cooperative Agreement between the Department of Health and Colleges and Universities</td> </tr> <tr> <td style="padding: 2px;">Incident Reporting Policy, Forms and Instructions</td> </tr> <tr> <td style="padding: 2px;">Initiation of Services</td> </tr> <tr> <td style="padding: 2px;">Instructions for Initiation of Services</td> </tr> <tr> <td style="padding: 2px;">Standard Third Party Networking Connection Agreement</td> </tr> <tr> <td style="padding: 2px;">Third Party Network Connection Request</td> </tr> <tr> <td style="padding: 2px;">Transmittal Letter Suggested Language</td> </tr> </table>	Acceptable Use and Confidentiality Agreement	Authorization for Non-Routine Disclosure of Protected Health Information	Cooperative Agreement between the Department of Health and Colleges and Universities	Incident Reporting Policy, Forms and Instructions	Initiation of Services	Instructions for Initiation of Services	Standard Third Party Networking Connection Agreement	Third Party Network Connection Request	Transmittal Letter Suggested Language	97
Acceptable Use and Confidentiality Agreement											
Authorization for Non-Routine Disclosure of Protected Health Information											
Cooperative Agreement between the Department of Health and Colleges and Universities											
Incident Reporting Policy, Forms and Instructions											
Initiation of Services											
Instructions for Initiation of Services											
Standard Third Party Networking Connection Agreement											
Third Party Network Connection Request											
Transmittal Letter Suggested Language											
Appendix C	Confidentiality Statues, Rules, and Federal Regulations	98									
Appendix D	Virus Protection	101									
Appendix E	Password Construction	104									
Appendix F	Disclosure of Special Reasons	105									

This page was left blank intentionally

I. Policy

State information resources are valuable assets of the State of Florida and its citizens and must be protected from unauthorized modification, destruction, disclosure (whether accidental or intentional), or use. The acquisition and protection of such assets is a management responsibility.

The Information Resource Security Program or Information Technology Security Program must prevent, detect, contain, and correct security violations. The program must also be responsive and adaptable to changing environments, vulnerabilities, and technologies affecting state information resources.

The information security policies and standards apply to all the Department of Health (DOH) workers which include employees, contractors and volunteers. They apply to all information systems that access, process, or have custody of data including automated information systems. They apply to mainframe, minicomputer, distributed processing, and networking environments of the state. They apply equally to all levels of management and to all personnel. They apply to information resources owned by others, such as political subdivisions of the state or agencies of the federal government, in those cases where the state has a contractual or fiduciary duty to protect the resources while in the custody of the state. In the event of a conflict, the more restrictive security measures apply.

Deviations from the DOH Information Security and Privacy policy may be requested by submitting to the State Surgeon General justification which must include an associated risk analysis and proposed physical, administrative and technical safeguards.

Each DOH division, office, county health department (CHD), Children's Medical Services area offices (CMS), and the A. G. Holley Hospital must have written local information security and privacy procedures to ensure the security of information and protect confidentiality, data integrity, and access to information. These local procedures must conform to the DOH Information Security and Privacy Program requirements as reflected in these DOH Information Security and Privacy policies. These local procedures should include core security procedures required by the department and supplemental operating procedures necessary to implement established DOH policies and protocols. All procedures must be written in approved DOH format and must be reviewed annually and updated as appropriate.

II. Authority

- A. Public Law (P.L.), 104-191
- B. 45 Code of Federal Regulations (C.F.R.), Parts 160 and 164
- C. Florida Statutes (F.S.) section 282.318
- D. Florida Administrative Code (F.A.C) 60DD

III. Supportive Data:

Federal and state law, rules, and regulations referenced in [Appendix C](#).

VII. Signature Block with Effective Date

Signature on file	10/1/07
Ana M. Viamonte Ros, M.D., M.P.H. State Surgeon General	Date

VII. DefinitionsReferenced in [Appendix A, Definitions and Glossary](#).**VI. Protocol**

- A. Type of Protocol: Administrative
- B. Personnel

Directors/Administrators of the DOH divisions, offices, CHDs, CMS area offices, the A. G. Holley Hospital, and other staff designated as responsible for developing and updating the written local information security and privacy procedures and corrective action plans.

- C. Competencies
 - 1. Knowledge necessary to develop and maintain comprehensive information security and privacy policies, protocols, and procedures.
 - 2. Knowledge of federal and state statutes, rules, and regulations pertaining to security and privacy.
 - 3. Knowledge of records management practices including storage, retrieval, and disposition.
 - 4. Knowledge of established departmental policies and protocols related to security and privacy of information.
- D. Outcomes
 - 1. Information security and privacy policies, protocols, and procedures in approved DOH format which incorporate all elements of department policies and protocols.
 - 2. Written local operating procedures for implementation of information security and privacy policies and protocols.
 - 3. Documented procedure for reviewing and updating written procedures at least annually.

4. Documented procedure for monitoring compliance with the information security and privacy policies, protocols, and procedures at least annually and developing/implementing a corrective action plan as needed.

E. Areas of Responsibility

1. Designated staff responsible for developing local information security and privacy procedures.

2. Review at least annually and update as appropriate, the local information security and privacy procedures. These documents must be consistent with federal and state laws and rules. They must also be consistent with departmental policies, protocols, and procedures.

3. Ensure that information security and privacy policies, protocols, and procedures are accessible to management, supervisory staff, and other staff identified as responsible for implementation of these documents.

4. Monitor compliance with the information security and privacy policies, protocols, and procedures.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
AG Holley Hospital
Web Managers

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Each Department of Health (DOH) division, office, county health department (CHD), Children's Medical Services (CMS) clinic, and the A. G. Holley Hospital will classify data (or information) as **public information** in accordance with Florida Statutes, *except* for data/information specifically exempted from disclosure by state statute. All data/information which is exempt from disclosure by state statute or designated as confidential by federal law (including protected medical information) will be classified as **confidential information**.

II. Authority

- A. Public Law (P.L.), 104-191
- B. 45 Code of Federal Regulations (C.F.R.), Parts 160 and 164
- C. Florida Statutes (F.S.) section 282.318
- D. Florida Administrative Code (F.A.C) 60DD

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A, Definitions and Glossary](#).

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

All DOH workers, including contractors, and volunteers.

- C. Competencies

- 1. Knowledge of federal and state statutes, rules, and regulations pertaining to public records, exemptions from disclosure, and requirements for maintaining confidentiality of information.

2. Knowledge of established departmental policies and protocols related to security and privacy of information.

3. Knowledge regarding when legal counsel should be consulted.

D. Outcomes

1. All department data/information shall be properly classified as public information or confidential information in accordance with applicable state and federal laws and statutes.

2. All department workers shall be knowledgeable of the classifications of data/information and the proper handling of data/information while carrying out the responsibilities of their jobs.

3. Confidential or exempt information shall be accessible only to workers who are authorized by the agency on the basis of performance, responsibilities, or as authorized by law.

4. Data/information sets containing any confidential or exempt information shall be identified as such.

E. Areas of Responsibility

1. Designate staff responsible for classification of data/information at the department level to ensure consistent handling department-wide.

2. Designate staff responsible for development of local information security and privacy procedures for the proper handling of public and confidential information to ensure data integrity and security. Label confidential information as "confidential" where reasonable and practicable.

3. Monitor compliance with the information privacy policies, protocols, and procedures.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Medical Services Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

The State Surgeon General and each Department of Health (DOH) division, office, county health department (CHD), Children's Medical Services clinic (CMS), and the A. G. Holley Hospital director are responsible for the security and privacy of information within his/her jurisdiction. Each must designate key personnel with specific responsibility to coordinate the security and privacy of information. The identity of the designee(s) must be documented in the local information security and privacy procedures, and the responsibilities must be included in the position description.

II. Authority

Not Applicable

III. Supportive Data

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A, Definitions and Glossary](#).

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel:
 - 1. State Surgeon General
 - 2. Health Insurance Portability and Accountability (HIPAA) Privacy Officer
 - 3. HIPAA Privacy Complaint Officer
 - 4. Information Security Manager
 - 5. HIPAA Security Officer
 - 6. Directors and Administrators of DOH divisions, offices, CHDs, and CMS area offices.

7. Information Resource Owners
8. Local Information Security and Privacy Coordinators
9. Local HIPAA Reviewing Officer (physician)
10. Local Information Custodians
11. Local Information Technology (IT) Disaster Recovery Coordinator

C. Competencies

1. Knowledge and skills to reasonably safeguard protected health information from any use or disclosure (intentional or unintentional), to limit incidental uses of the information and insure a minimum disclosure of necessary protected health information.
2. Knowledge necessary to coordinate the implementation of information security and privacy policies, protocols, and procedures.
3. Knowledge of federal and state statutes, rules, and regulations pertaining to the security, privacy, and confidentiality of information.
4. Knowledge of patient's rights relating to information security and privacy.
5. Knowledge of program areas.
6. Assigned roles within the department to provide leadership.

D. Outcomes

1. Designation of personnel.
2. Documentation of personnel in local security and privacy procedures.
3. Documentation of responsibilities in position description(s).
4. Documentation of delegation(s) will be maintained by the local security and privacy program(s) and communicated to the proper DOH level.
5. Implementation of an agency security program that is compliant with all requirements of Section 282.318, F.S. and the HIPAA Security rule.

E. Areas of Responsibility

1. State Surgeon General

This person is ultimately responsible for the implementation of information security and privacy policies, protocols, and procedures. The State Surgeon General's responsibilities include designating headquarters' security officials (essential staff) as required by the HIPAA security rule and Florida Statutes. These include HIPAA Privacy Officer, HIPAA Privacy Complaint Officer, Information Security Manager, and the HIPAA Security Officer positions. The State Surgeon General documents duties and responsibilities in position descriptions and in specific delegation of authority including resource ownership.

2. HIPAA Privacy Officer

Responsibilities include:

- a. Serving as HIPAA privacy consultant to the organization for all departments and appropriate entities.
- b. Providing a leadership role to the agency for privacy oversight including development of policies and procedures, implementation and monitoring/corrective actions to ensure that DOH complies with federal, state, and agency privacy requirements.
- c. Providing leadership in the implementation and maintenance of privacy policies and procedures.
- d. Implementing through policy, the recommendations of the local security and privacy officers, legal counsel for security and privacy officers, and the agency privacy complaint officer.
- e. Overseeing privacy training and orientation to all employees, volunteers, medical and professional staff, and other third parties as appropriate.
- f. Ensuring that the organization has and maintains appropriate consent and authorization forms; notice of privacy practices and materials reflecting current organization; and legal practices and requirements.
- g. Developing and implementing information privacy risk assessments and in coordination with the agency privacy complaint officer, conducts related ongoing compliance monitoring.
- h. Working cooperatively with the legal counsel, the privacy officers, and other applicable organizational units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.
- i. Initiating, facilitating and promoting activities to foster privacy awareness within the organization and related entities.

j. Reviewing all system-related information security plans throughout the organization's network to ensure the security and privacy of protected health information; acts as a liaison to the information systems department and security officers.

k. Maintaining current knowledge of applicable federal and state privacy laws and standards; monitors advancements in technologies to ensure organizational adaptation and compliance in coordination with the information technology unit and security officers.

3. HIPAA Privacy Complaint Officer

The DOH Inspector General functions as the agency's privacy complaint officer and will serve as a point of contact for all complaints of privacy violations.

Responsibilities include:

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

b. Conferring with the appropriate privacy official and unit director/administrator on all complaints.

c. Responding to inquiries from the general public regarding the content of the Notice of Privacy Practices.

4. Information Security Manager (ISM)

The ISM will be responsible for administering the department's Data and Information Technology Resource Security Program, as required by Florida Statutes and as further delegated by the State Surgeon General.

5. HIPAA Security Officer

The HIPAA security officer will be responsible for administering the department's Data and Information Technology Security Program and the requirements in the HIPAA Security Rule.

6. Directors/Administrators of DOH divisions, offices, CHDs, CMS clinics, and the A. G. Holley Hospital.

These positions will be located in each DOH division, office, CHD, CMS clinics, and the A.G. Holley Hospital. Responsibilities include:

a. Designating, as applicable, essential staff for the local information security and privacy coordinators, local HIPAA reviewing officer (physician), local information custodian, and local IT disaster recovery coordinator positions.

b. Notification of personnel appointed to these positions will be reported to the HIPAA privacy officer and ISM within ten days of this policy becoming effective. Subsequent changes will be reported to the same individuals within ten days of the effective date of the change.

7. Local Information Security and Privacy Coordinators

These positions will be located in each DOH division, office, CHD, CMS clinics, and the A.G. Holley Hospital. Responsibilities include:

- a. Reviewing and familiarization with the contents of the respective statutes, administrative code, departmental policies, protocols and procedures relating to information security and privacy; and maintaining these documents in a way which assures that they are current.
- b. Maintaining professional skills and competencies by participating in training and other professional development activities.
- c. Communicating with the DOH ISM and privacy officer to ensure a uniform approach to security and privacy throughout the department.
- d. Coordinating the Information Security and Privacy Program in all locations within the information security and privacy coordinator's jurisdiction and acting as a central point of contact for other staff that are assigned information security and privacy duties to ensure a uniform approach to security and privacy.
- e. Coordinating the development of local information security and privacy procedures.
- f. Coordinating the review and update of the local information security and privacy procedures at least annually.
- g. Providing access to the information security and privacy policies, protocols, and procedures to staff.
- h. Coordinating the procurement and dissemination of current information security and privacy awareness training materials consistent with DOH policy and protocols.
- i. Ensures that formal training is available at least annually to all employees (Refer to Information Security Policy 5: Security and Privacy Awareness Training).
- j. Ensuring that all new employees have completed security and privacy awareness training within 30 working days of employment and/or prior to accessing confidential information, whichever is earliest (refer to

Information Security Policy 5: Security and Privacy Awareness Training).

k. Coordinating an information security and privacy risk assessment annually (refer to DOHP 50-10l-07 Information Security and Privacy Policy 13: Risk Analysis).

l. Coordinating follow-up of corrective action as determined by the information security and privacy risk assessment.

m. Participating in performance improvement reviews.

n. Monitoring adherence to the protocols and procedures for secured areas (see DOHP 50-10e-07 Information Security and Privacy Policy 6: Secured Areas and Physical Security Procedures section VI.E.2). Coordinate corrective actions as appropriate.

o. Monitoring the list of staff authorized to access confidential information and facilitating corrections as appropriate (see DOHP 50-10e-07 Information Security and Privacy Policy 6: Secured Areas and Physical Security Procedures section VI.E.2).

p. Monitoring the assignment and maintenance of user codes and login names for all applications within his/her jurisdiction by reviewing the list of persons with access to electronically stored data and facilitating changes as appropriate.

q. Maintaining incident reports and documentation of resolution of all suspected and confirmed breaches of security and confidentiality (refer to DOHP 5-6-06 Incident Reporting Policy and Procedures). Coordinating and monitoring corrective action identified during the investigation of an incident or risk analysis.

r. Assisting the local systems administrator with maintenance, training and annual testing of the site's Information Technology Disaster Recovery Plan (refer to DOHP 50-10m-07 Information Security and Privacy Policy 14: Contingency Planning).

8. Local HIPAA Reviewing Officer (physician)

This person will be a licensed healthcare professional who holds a valid license in Florida identified as a potential reviewing official for each of the covered units. A reviewing official is designated by the local privacy officer after consultation with the director or administrator of the covered unit, CHD or CMS clinic. The reviewing official does not need to be located administratively within the organizational unit for which they have been designated. 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).
- b. The reviewing official cannot have been directly involved in the original decision to deny access.

9. Local Information Custodian

This person is responsible for the activities related to specific information sets for which authority has been delegated. Responsibilities include:

- a. Establishes procedures in accordance with DOH policies, protocols, and procedures to ensure information is accessible only to authorized persons.
- b. Delegates authority to assist with information custodian duties. This delegation must be documented.
- c. Maintains authorized access to the information set(s).
- d. Reviews and initials the access log for secured areas at least monthly.
- e. Establishes local procedures in accordance with DOH policies.
- f. Implements controls specified by information resource owners.
- g. Assists owners in evaluating the cost-effectiveness of controls and monitoring.
- h. Implements and monitor techniques and procedures for reporting incidents.

10. Information Resource Owner

- a. Agency managers who are responsible for specifying the security properties associated with the information their organization possesses and are responsible for the integrity and accuracy of that information.
- b. Owners of information resources 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. These controls shall selectively limit services based upon user identification and authentication or designation of other users, including the public where authorized, as a class (i.e., public access through dial-up or public switched networks) for the duration of a computer session.

- c. Network access to an application containing confidential or exempt data and data sharing between applications, shall be as authorized by the application owners and shall require authentication.
- d. Develop and test cost-effective disaster preparedness plans for all functions identified as critical to the continuity of governmental operations. These plans will provide for the prompt and effective continuation of critical state missions in the event of a disaster.

11. Local IT Disaster Recovery Coordinator

The local IT disaster recovery coordinator is the person in the local office who is responsible for planning and directing the detailed information technology activities before, during, and after the disaster. The local IT disaster recovery coordinator is usually the lead system administrator, but could be the management information systems (MIS) director, other local IT staff, the local office director, the local office administrator, or the local Continuity of Operations Plan (COOP) coordinator if that person is the best person to perform the role. The regional disaster preparedness consultant will generally provide considerable assistance completing the Continuity of Operations Plan for Information Technology (COOP-IT) and performing some of the other responsibilities of local disaster preparedness. The disaster preparedness consultant should not be designated as the local IT Disaster Recovery Coordinator (refer to DOHP 50-10n-07 Information Security and Privacy Policy 15: Contingency Planning and the template for COOP-IT, version 2).

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in

August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Department of Health (DOH) workers shall be held accountable for protecting information from unauthorized modification, destruction, use or disclosure, and for safeguarding confidential information. All DOH data, information, and technology resources shall only be used for official state business, except as allowed by the department's policy, protocols, and procedures. This includes information in any format.

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 approved software and hardware will be installed.

DOH workers having access to computer-related media are expected to know the department's information security and privacy policies, protocols, and procedures. They are to conduct their activities accordingly. An "Acceptable Use and Confidentiality Agreement" must be signed by each DOH worker and filed at the local level. This document confirms that the worker understands the requirements and penalties for failure to comply with the department's information security and privacy policies, protocols, and procedures.

II. Authority

See [Appendix B](#), *Acceptable Use and Confidentiality Agreement*.

III. Supportive Data

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

A. Type of Protocol: Administrative

B. Personnel

All DOH personnel including volunteer employees and contractors accessing our data and information resources.

C. Competencies

1. Knowledge and skills to reasonably safeguard confidential information from any intentional or unintentional use or disclosure.
2. Knowledge of DOH policies, protocols, and procedures related to information security and privacy.
3. Knowledge of information classified as confidential or exempt from public record disclosure in federal regulations and state laws and rules, requiring specific actions to safeguard.
4. Knowledge of information technology resources security and practices.

D. Outcomes

1. This Acceptable Use and Confidentiality Agreement, DOH form DH1120 (refer to [Appendix B-Forms](#)), will be completed by a DOH worker prior to providing services to patients, accessing confidential information, accessing information technology resources, or within 30 days of the employment start date; whichever is earliest.
2. Completed Acceptable Use and Confidentiality Agreement is maintained locally.
3. Appropriate security controls are in place to mitigate risks of using mobile devices.
4. DOH workers utilize IT resources in a manner that safeguards those resources.

E. Areas of Responsibility

1. All DOH workers with access to confidential information must sign Section A of the Acceptable Use and Confidentiality Agreement, DOH form DH1120 (refer to [Appendix B-Forms](#)).
2. All DOH workers having access to DOH Information Technology Resources must sign Section B of form DH 1120.
3. The signed DOH form DH 1120 must be maintained at the local level. This document shall be signed by the DOH worker and witnessed by another DOH worker.
4. All members of the DOH worker will have access to the respective Florida Statutes, administrative rules, and the DOH policies, protocols, and procedures.

VII. Procedure**A. General**

1. The Florida Computer Crimes Act, Chapter 815, F.S., prohibits the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information, and the stealing of data from computer files. Computer crimes violate the department's policies and may also result in criminal charges. Workers who work with computers or have access to computer information are to be familiar with Chapter 815, F.S.; the DOH Information Security and Privacy policies, protocols, procedures; in addition to the Health Insurance Portability and Accountability Act (HIPAA) legislation. Workers should ask their supervisor for any needed clarification. DOH workers found to have violated these policies, laws, regulations, etc., may be subject to disciplinary action, up to and including termination of employment.

2. Supervisors may monitor computer use by direct observation, review computer history files through the systems administrator, or review work productivity and quality.

a. The local system administrator, with management approval (Director/Administrator or local HR Director), can look at an employee's computer cookies, Internet history, and event logs for evidence of what the supervisor has observed, suspects, and/or was notified occurred and supply the manager with information (screen shots, printouts of files, a written report).

b. If additional information is needed, the supervisor must have the Office of the Inspector General or the Headquarters Office of Human Resources contact the Bureau of Strategic Information Technologies, Security Administration Team and request the information be released.

3. Use of streaming media technologies can only be used with prior written approval of the user's supervisor and the Chief Information Officer (CIO) or delegate.

4. Access to the Internet or email service is a privilege, not a right. Workers must adhere to state policies, department policies and procedures, federal regulations, and state and local laws.

5. DOH workers shall have no expectation of privacy when using DOH resources.

6. The Security Administration Team and Root Administrator staff will have the capability to monitor all devices on the DOH network.

7. The department may inspect any and all files stored on any network or local computer system, including removable media.
8. Use of state resources constitutes consent to monitoring activities with or without a warning.
9. Only DOH-managed devices may be connected to the DOH network. Exceptions must be granted in writing by the Information Security Manager (ISM) and CIO.
10. Only agency-approved software shall be installed on agency-owned or agency-managed computers.
11. DOH devices (including computers, mobile devices) will be configured according to IT-approved standards and guidelines.
12. Illegal duplication of software is prohibited.
13. Each computer user must report suspected computer malware (viruses, etc.) occurrences to the local system administrator or designee immediately.
14. DOH workers may use the department's Internet email access link for agency email access while away from the office with their supervisors' approval.
 - a. Included DOH workers (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 and must record any additional hours as required by department policy.
 - b. DOH workers must insure that the computer used for Internet email access has up-to-date anti-malware software and current operating system security patches.
 - c. Approval to use Internet email access in no way eliminates the requirement for prior approval for telecommuting in accordance with the Telecommuting Policy and Procedures (DOHP 60-24-06)
http://dohiws.doh.state.fl.us/divisions/administration/Personnel/Policies/Telecommute_60-24-06.pdf

B. Computer Use

1. DOH workers will be given a user account to access DOH information technology resources. This access will be based on the documented need as provided by the appropriate hiring authority. The DOH CIO or delegate has final authority regarding access to the DOH network and IT resources. Supervisors will regularly review the access privileges of staff and ensure access is appropriate to job responsibilities. Workers who have or are responsible for a user account within the department's network are responsible for taking the

appropriate steps to select and secure their passwords (refer to [Appendix E](#), Password Construction).

- a. Access to agency information technology resources is reserved for agency-approved users.
 - b. Agency computer users shall have unique user accounts.
 - c. Agency computer users shall be held accountable for their account activities.
 - d. User accounts must be authenticated at a minimum by a password.
 - e. Agency computer users are responsible for safeguarding their passwords and other authentication methods.
 - f. Agency workers must not share their agency account passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.
 - g. Agency workers shall immediately report suspected account compromises according to agency incident reporting procedures.
 - h. Agency workers shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency incident reporting procedures.
 - i. All user-level passwords must be changed every 30 days.
 - j. Passwords should not be inserted into e-mail messages or other forms of clear text (plain text) messaging. Passwords should be encrypted or secured by other means when delivered by the system administrator to the users.
 - k. Passwords should be at least eight alphabetic and numeric characters in length.
2. DOH workers must not disable, alter, or circumvent agency workstation security measures.
 3. DOH workers must logoff or lock their workstations prior to leaving the work area.
 4. Workstations must be secured with a password-protected screensaver with the automatic activation feature set at no more than 10 minutes.

5. Access to agency information technology resources is reserved for agency business purposes.
6. DOH workers are permitted to briefly visit non-prohibited Internet sites or use e-mail for personal reasons during non-work hours (lunch period or before/after work) subject to the limitations contained within this policy.
 - a. Usage must not interfere with the worker's job duties.
 - b. Usage must not consume significant amounts of DOH IT resources or compromise the normal functionality of the department's systems.
 - c. Personal use must not result in any additional cost to the department.
 - d. Personal use may be monitored and subject the employee to disciplinary action.
 - e. DOH workers may access non-DOH browser based email accounts such as AOL, Yahoo, Hotmail, etc. 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-DOH email.
 - f. Examples of non-prohibited Internet/Intranet sites are those dealing with health matters, weather, news, business or work-related topics, community activities, career advancement, and personal enrichment.

C. Mobile Computing

1. Mobile computing devices will be issued to and used by only DOH-authorized users.
2. Mobile computing devices will require user authentication.
3. Mobile computing devices shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.
4. Mobile computing devices must use current and up-to-date anti-malware software where possible.
5. Mobile computing devices must activate an agency-approved personal firewall (where technology permits) when connected to a non-DOH network.

6. When connecting a DOH laptop to a non-DOH network, the DOH worker must immediately activate an approved DOH Virtual Private Network (VPN) connection.
7. Workers must take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
8. Mobile device users must report theft of mobile devices immediately to appropriate personnel per DOHP 250-4-04-Insurance Claims Reporting Policy and Procedures and DOHP 5-6-06 Incident Reporting Policy and Procedures. In addition the DOH Information Security Manager and State Office of Information Security must be notified.
9. Only DOH mobile storage devices may store department data.
10. All data residing on DOH mobile computing devices and mobile storage devices is the property of the department and subject to monitoring and public records law.
11. Mobile computing devices used with confidential information require whole drive encryption.
12. Mobile storage devices with confidential data must have encryption technology enabled such that all content resides encrypted.
13. To prevent loss of data, DOH data stored on mobile devices must be backed up.
14. Data, including e-mail, on mobile devices that is no longer needed must be purged as often as possible.

D. Unacceptable Uses

1. The prohibited activities listed below are examples and are not all inclusive. DOH workers 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.
2. DOH workers must not use DOH IT resources for any purpose which violates state or federal laws or rules.
3. DOH IT resources must not be used for personal profit, benefit, or gain.
4. DOH IT resources must not be used for political campaigning.
5. DOH workers must not install, introduce, download, access, or distribute:

- a. Software not approved by the DOH Information Technology Standards Workgroup (ITSW).
 - b. Software not licensed to the department or its affiliates.
 - c. Viruses, worms, Trojan horses, e-mail bombs, etc., through willful intent or negligence. Note: files downloaded from the Internet should be scanned for viruses before use and/or distribution; no file received from an unknown source should be downloaded even if attached to an e-mail message or downloaded from the Internet.
 - d. Harassing, intimidating, threatening, complaining, or otherwise annoying materials including chain letters (chain letters may include any emails, Intranet or Internet that ask or advise the recipient to forward the e-mail to more than one other person).
 - e. Sexually explicit, pornographic, or vulgar material.
 - f. Inappropriate language or profanity, including, but not limited to obscene or inappropriate language, racial, ethnic, or other discriminatory content.
 - g. Non-work related material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, or violence.
 - h. Non-work related chat rooms, news groups, political groups, singles clubs, dating services, computer hacker websites, or software.
 - i. 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). Recognition of employment or retirement and ceremonies for employee award programs are state business related functions.
6. DOH workers must not respond directly to the originator of offensive electronic messages. DOH workers should report the communications to their supervisor, the Information Security Coordinator and, if necessary, to the DOH Office of Inspector General.
 7. DOH workers must not program DOH email to automatically forward messages to a non-DOH email address.
 8. DOH workers must not create security breaches or otherwise disrupt network communication. 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.

9. DOH workers must not utilize port scanning, security scanning, and unauthorized executing any form of network monitoring which will intercept data not intended for the employee.
10. Non-DOH devices (including personal MP3 players, thumb drives, printers) shall not be connected to DOH systems without CIO authorization.
11. DOH workers must not attempt to access information or resources without authorization.
12. DOH workers must not use DOH IT resources for any activity which adversely affects the availability, confidentiality, or integrity of DOH or state information technology resources.

VIII. Distribution List

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

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Department of Health workers will receive an initial security and privacy awareness training prior to providing services to clients, accessing confidential information, accessing information technology, or within 30 days of employment start date, whichever is earliest. The training course can be presented one-on-one, as a self-study, or as a formal training course. Regardless of format, the initial training must cover the items outlined in the core training protocol and other essential job-specific training as required by position responsibilities. In addition to the initial training, all employees and volunteers shall receive information security and privacy awareness update training at least annually. Documentation of training shall be maintained at the local level and shall be accessible to supervisory personnel.

Information security and privacy awareness training curriculum and materials shall be consistent with federal regulations, state laws and rules, as well as departmental policies, protocols, and procedures. Training materials and curriculum shall be reviewed at least annually and updated as appropriate.

II. Authority

See [Appendix B](#), *Acceptable Use and Confidentiality Agreement*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date**V. Definitions**

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

A. Type of Protocol: Administrative

B. Personnel

All DOH personnel, including contractors, and volunteers.

C. Competencies

1. Knowledge necessary to effectively coordinate and present training.
2. Knowledge of DOH policies, protocols, and procedures related to information security and privacy and release of information.
3. Knowledge of operating procedures for securing information.
4. Knowledge of applicable federal regulations, state laws, rules, and regulations regarding confidential information.

D. Outcomes

1. Initial information security and privacy awareness training is provided prior to employee having access to clients, confidential information, accessing information technology, or within 30 days of employment, whichever is earlier.
2. Information security and privacy awareness training updates are provided at least annually to all staff.
3. Documentation of core information security and privacy awareness training is maintained at the local level.
4. Information security and privacy awareness training materials and curriculum are consistent with federal regulations, state laws and rules, as well as departmental policies, protocols, and procedures.

E. Areas of Responsibility

The local Information Security and Privacy Coordinators are responsible to ensure the awareness and training program includes the following topics:

1. Overview of state and federal security and privacy laws, rules, and regulations.
2. Overview of DOH Information Security and Privacy Policy.
3. Overview of personnel disciplinary actions and legal consequences for information security and privacy policy violations.
4. Procedures for reporting information security and privacy incidents.
5. Documentation of individuals who have completed security and privacy awareness training. This documentation will be maintained locally.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Department of Health (DOH) divisions, offices, county health departments (CHDs), Children's Medical Services (CMS) clinics and the A. G. Holley Hospital must designate and maintain secured areas to ensure the security and privacy of information and information technology resources; to protect confidentiality and data integrity; and to provide appropriate access to information using administrative, physical, and technical controls. Each designated secured area shall be documented in the local information security and privacy procedures.

II. Authority

See [Appendix C](#), *Summary of Confidentiality statutes Shielding Documents in the Custody of the Department of Health*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

A. Type of Protocol: Administrative

B. Personnel

All Directors/Administrators of DOH divisions, offices, CHDs, CMS area offices, and the A. G. Holley Hospital 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 and state statutes, rules and regulations pertaining to physical security requirements, public records, exemptions from disclosure, and requirements for maintaining confidentiality of information.

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

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

D. Outcomes

1. All confidential information is maintained in a secured area.

2. Client privacy is maintained.

3. Employee privacy is maintained.

4. The integrity of data is protected.

5. Information exempt from public record disclosure is handled in a confidential manner.

6. Access to confidential information will be limited to those with a documented "need to know."

7. Information technology resources will be protected against alteration, disclosure, and destruction.

E. Areas of Responsibility

1. A secured area has a reliable locking system. Doors will be securely locked at all times when no one is in the secured area. Windows, walls, floors, or ceilings do 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.

c. Security is achieved by physical, administrative, and technical controls.

2. A secured area has access limited to a documented list of authorized personnel.

3. A key custodian and an alternate key custodian will be designated for each secured area to document and manage physical access to the secured area.

- a. Documentation will be maintained for the number of keys distributed. No key shall be provided for persons not on the list of personnel with authorized access.
 - b. Documentation will include the signature of the person receiving the key.
4. An access log will be kept and maintained for the secured area.
 - a. Persons who may have temporary or occasional authorized access, but are not on the list, will record their signature, date, time in and out, the purpose of entering the room, and description of any items taken from the secured area.
 - b. Persons with temporary or occasional authorized access shall be escorted at all times.
5. An inventory of resources and information sets maintained in the designated secure area will be updated at least annually.
6. Procedures for removing information from the designated secured area will be documented and monitored.
7. Computer rooms are secured areas. Physical controls shall be appropriate for the size and criticality of the information technology resources within a secured area.
 - a. Management reviews of physical security measures shall be conducted annually and whenever facilities or security procedures are modified or compromised.
 - b. New and remodeled DOH computer rooms must be constructed so that they have reasonable protection against fire spread, water damage, vandalism, and other potential threats.
 - c. Information resources shall be protected from environmental hazards; in accordance with manufacturer's specifications.
 - d. All computers must be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers in accordance with DOH Information Technology Standards.
8. Repairs and modifications to secured area housing electronic information systems shall be documented and maintained for six years in accordance to 45 CFR 164.105 (c) (2).

VII. Procedure

Applicable standard operation procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

All information/data which is exempt from disclosure by state or federal law, rule, or regulation is confidential. Each Department of Health (DOH) division, office, county health department (CHD), Children's Medical Services (CMS) clinic, and the A. G. Holley Hospital will classify information/data sets in their custody as confidential or not confidential. Confidential information must be secured using appropriate administrative, technical, and physical safeguards. It is the responsibility of each DOH worker to maintain the confidentiality of information/data.

II. Authority

- A. 45 Code of Federal Regulations (C.F.R.), Parts 160 and 164
- B. Florida Statutes (F.S.) section 282.318
- C. Florida Administrative Code (F.A.C) 60DD

See [Appendix C](#), *Summary of Confidentiality Statutes Shielding Documents in the Custody of the Department of Health*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

/s/ Signature on file

November 25, 2008

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

All DOH workers, employees, contract and exempt employees, and volunteers with access to confidential information.

- C. Competencies
 - 1. Knowledge of information classified as confidential.

2. Knowledge of federal and state laws, rules, and regulations pertinent to maintaining patient medical information.
 3. Knowledge of DOH policies, protocols, and procedures.
 4. Knowledge of operating procedures for mailing protected information.
 5. Knowledge of procedures necessary to keep confidential information secured while providing patient care services.
- D. Outcomes
1. Confidential data sets are identified and protected using appropriate administrative, technical, and physical safeguards.
 2. Integrity of data sets is maintained and is incorporated within information security and privacy protocols, and procedures.
- E. Areas of Responsibility
1. General
 - a. The DOH Office of General Counsel shall maintain a reference list of state and federal statutes and rules relevant to agency confidential information.
 - b. Audit logs of access and modifications to confidential information should be maintained.
 - c. The Information Security and Privacy Coordinators shall be granted access to review audit logs containing accountability details regardless of format.
 - d. Agreements and procedures shall be in place for sharing, handling, or storing confidential data with entities outside the agency.
 - e. All DOH workers shall be knowledgeable of the classifications of data/information and the proper handling of data/information.
 - f. Confidential information shall be accessible only to authorized persons.
 - g. Confidential information transferred externally on paper or electronic media must be protected.
 - h. Information with employee identifiers, client identifiers, or other confidential content is not left unattended or unsecured.

-
- i. Unauthorized persons will be escorted and not left unattended in secured areas.
 - j. Position computer monitors to prevent unauthorized viewing.
 - k. Consultations involving confidential information must be held in areas with restricted access.
 - l. Confidential information must be printed using appropriate administrative, technical, and physical safeguards that prevent unauthorized viewing.
 - m. Electronic transmission of confidential information must be encrypted.
 - n. Person(s) having the authority to perform electronic file transfers (including facsimile) of confidential information will be documented in the local operating procedures.
 - o. Data backups must be locked in a secured area.
 - p. Proper authorization to disclose patient medical information must be obtained prior to disclosure (refer to Information Security and Privacy Policy 8: Disclosure of Patient Medical Information).
2. Maintaining Confidential Information—Communications
- a. Telephone Information
 - (1) Confidential information is discussed by phone only in areas where the conversation cannot be overheard.
 - (2) DOH workers must determine identification of the caller and what information can be disclosed.
 - (3) Cellular phones (including the Blackberry) 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.
 - b. Mailing Information
 - (1) A secured mail intake site must be used to receive incoming confidential information such as laboratory results, patient medical records, and surveillance case reports.
 - (2) Mailrooms and mailboxes must be secured to prevent unauthorized access to incoming and outgoing mail.

(3) Double enveloping is required when mailing confidential or sensitive information. The outside envelope is addressed to the recipient. The inside envelope is marked confidential and specifies the recipient.

c. Facsimile Information

(1) Confidential information may be faxed using appropriate administrative, technical, and physical safeguards. Patient medical information may be faxed for the purpose of treatment (including diagnosis) of the patient, payment processing, healthcare operations, or with specific authorization from the client

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

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

(4) 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."

d. Electronic Mail (E-mail)

Electronic transmission of confidential information must be encrypted when the transport medium is public or the transport medium is not owned or managed by the department.

3. Clinic Procedures—General

a. Telephones shall be answered in a manner that does not identify clinic specialty.

b. Registration and financial eligibility determination interviews take place in areas that do not compromise client confidentiality.

-
- c. Client names shall not be called in any specialty clinics.
 - d. Sign-in logs may be used in general clinic settings only. Information collected is restricted to client name and arrival time.
 - e. The exterior of a hard copy patient medical record shall not be flagged to identify information other than known allergies to specific medications or name alert.
 - f. Records shall not be stored in a manner that would distinguish them from any other record.
 - g. Clients shall not be unattended in restricted areas.
4. Clinic Procedures—Appointment Reminders
- a. The client's preferred method of contact is documented in the client's medical record. Appointment reminders are discussed with the client at their first visit. If a client has given consent to be contacted by phone, cell phone or pager; staff may leave messages stating only the date and time of the appointment. For numeric pagers, only the phone number is listed.
 - b. Specialty clinic identifiers are not permitted on client communication envelopes. 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.
 - c. Patients can complete their own reminder postcards at the time of their visit, which may be sent by U.S. mail.
 - d. Client communications such as appointment scheduling, and appointment reminder procedures must be handled in a manner that does not compromise client's confidentiality. These procedures must not identify specific services or clinics.
5. Maintaining Confidential Information—Field Security
- a. Confidential information shall be transported only by persons authorized in position descriptions or as authorized by law.
 - b. DOH workers must sign out all information removed from the secured area.
 - c. Sign-out documentation must be retained by the information custodian in accordance with the record retention and disposition schedule developed by the department.

- d. Confidential information carried into the field is limited to the minimum required to perform responsibilities.
- e. Prior permission must be obtained if information will not be returned by the close of same business day.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was last revised in October 2008 and supersedes earlier versions. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Confidential information shall not be disclosed without proper authority as outlined in the protocols included in this document. Local operating procedures shall be established to ensure that protected information is released only in accordance with these protocols.

II. Authority

See Appendix B.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in the following text and Appendix C.

IV. Signature Block with Effective Date

/s/ Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

November 25, 2008

Date

V. Definitions

Referenced in Appendix A, *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Workers

All Department of Health (DOH) workers 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 regulations, state laws, and rules pertinent to the disclosure of confidential information.
3. Knowledge of DOH policies, protocols, and procedures related to the disclosure of confidential information.

4. Knowledge of the appropriate elements that constitute a proper authorization to disclose confidential information.
5. Knowledge of the circumstances in which confidential information may be disclosed without the consent of the person to whom the information pertains.
6. Knowledge and skills to reasonably safeguard confidential information from any intentional or unintentional use or disclosure; insure minimum necessary use and disclosure; and limit incidental uses and disclosures of the information.
7. Knowledge of patient's rights.

D. Outcomes

1. Security and privacy of client information is maintained.
2. Authorized workers will disclose confidential information only after proper authorization has been obtained.
3. Information that is exempt from public record disclosure is maintained in a confidential manner.

E. Areas of Responsibility

1. Disclosure of Confidential Information

Information/Data exempt from public disclosure by state or federal law, rule, or regulation is confidential.

The implementation of confidentiality laws primarily affecting the department is as follows:

a. Personnel record entries

Information maintained in the personnel files of state workers is generally accessible by the public with certain exceptions including the following:

- (1) Social Security numbers are not releasable in any record, including personnel records, with the exception of medical treatment records which rely on social security numbers as an identifier for the performance of legally prescribed duties and responsibilities (reference sections 119.071(4) (a) and 119.071(5)(a)2., Florida Statutes).
- (2) Location information including but not limited to home addresses; telephone numbers; social security numbers; photographs; daycare information; of the spouse; children of current or former justices; circuit and county court judges; state

attorneys; assistant state attorneys; statewide prosecutors or assistant statewide prosecutors; law enforcement officers; code enforcement officers; firefighters certified in accordance with Section 633.35, Florida Statutes; Department of Children and Families' (DCF) abuse investigators; department personnel supporting abuse investigations; human resource; labor relations, or employee relations directors; assistant directors; managers or assistant managers of any government agency; and the identity of any individual providing his or her name for ridesharing, is confidential and not disclosable from department personnel records (reference section 119.071(4)(d), Florida Statutes).

(3) Complaints of discrimination relating to race, color, religion, sex, national origin, age, handicap, or marital status are confidential and not disclosable (reference section 119.0711(1), Florida Statutes).

(4) Medical information pertaining to a prospective, current, or former officer or employee of an agency is confidential and not disclosable (reference section 119.071(4) (b), Florida Statutes).

b. Contracting

Sealed bids or proposals received by the department are not disclosable until the award date or 10 days after opening whichever is first (reference section 119.071(1)(b), Florida Statutes).

Financial statements received by the department for bid pre-qualifying are confidential and not disclosable (reference section 119.071(1)(c), Florida Statutes).

c. Client Eligibility Applications

All personal identifying information, bank account numbers, debit, and credit card numbers contained in records relating to an individual's personal health or eligibility for health-related services are confidential and not disclosable (reference section 119.0712(1), Florida Statutes).

d. Computer software

Licensed commercial and proprietary computer programs and data processing software are confidential and not disclosable (reference section 119.071(1) (f), Florida Statutes).

e. Patient Medical Information Disclosure

Healthcare providers may share patient medical information without the patient's authorization for the purpose of treating that patient (reference section 456.057(7) (a), Florida Statutes, and 45 CFR 164.506(c) (2)).

(1) Written Authorization to Disclose Patient Medical Information

Readily identifiable patient medical information will be disclosed as directed in a written document, signed within 12 months (unless otherwise specifically authorized in the document) by the patient or authorized representative, providing HIV test results, psychiatric, psychological or psychotherapeutic records, Women, Infants and Children (WIC), and substance abuse service provider client records are specifically authorized for disclosure.

(a) Except when the disclosure is to another healthcare provider for treatment or diagnosis, HIV testing and results require a specific authorization stating the HIV test result may be disclosed to a specific person or organization (Section 381.004(3), Florida Statutes). The HIV test result disclosure transmittal document will include a warning: "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" except in the hospital setting with specific written informed consent (Reference Sections 381.004(3) (e), (f) and (g), Florida Statutes).

(b) STD investigatory and contact tracing records require specific authorization to disclose. (Reference Section 384.29, Florida Statutes.) Individual patient STD medical records may be disclosed in accordance with requirements of general patient medical information. (Reference Section 456.057, Florida Statutes.)

(c) TB investigatory and contact tracing records require specific authorization to disclose. (Reference Section 392.65, Florida Statutes.) Individual patient TB medical records may be disclosed in accordance with requirements of general patient medical information. (Reference Sections 456.057 and 395.3025, Florida Statutes.)

(d) Psychiatric, psychological or psychotherapeutic notes made under the authority of a mental health provider licensed under Chapter 490 or 491, Florida Statutes, may be supplied in a report form at the discretion of the psychiatrist, psychologist or psychotherapist. If written request or complete copies of the record is made for the use of a subsequent licensed mental health provider the complete record shall be provided (Reference Section 456.057(6), Florida Statutes and 45 CFR 164.508(a) (2)).

(e) Substance abuse service provider client records, maintained by the department shall not be disclosed except on the specific written authorization of the patient (Reference Section 397.501(7), Florida Statutes, and 42 CFR Part 2).

(2) Minor Child Medical Services

(a) When a parent or guardian consents for medical services on behalf of a minor, the patient medical information may be disclosed to the parent or guardian.

(b) When a minor is authorized and does consent for medical services, only the minor may authorize disclosure of the patient medical information (Reference 45 CFR 164.502(e) (3)).

(c) Treatment for STD, family planning, and substance abuse have statutory provisions authorizing minor children to consent to medical treatment under certain circumstances (Reference Sections 384.30, 381.0051, and 397.501, Florida Statutes, respectively).

(3) Subpoenaed Medical Records

General patient medical information records excluding public health investigatory records, HIV test results, substance abuse service provider client record, and WIC records may be disclosed under the authority of a subpoena providing the patient or patient's authorized representative has had an opportunity to object and has not. This opportunity to object may be established by a copy of the notice to issue the subpoena for medical records, a signed representation of the requesting attorney that an opportunity to object has occurred and no objection has been received or the equivalent (Reference Section 456.057(7)(5), Florida Statutes, and 45 CFR 164.512(e)(1)(ii)(A)).

(4) Workers' Compensation Medical Records

Patient medical information of services provided for injury or illness specifically identified by the patient as work-related, with the exception of HIV testing and results, is disclosable to the employer, employer's workers' compensation insurance carrier, or the employer's attorney without written authorization of the patient. This disclosure is limited to records of services provided in the treatment of a specifically identified workplace injury or illness. (Reference Section 440.13(4) (c), Florida Statutes). WIC, substance abuse treatment, family planning, or other general

medical records are not to be disclosed under this provision unless patient clearly identified as work related.

(5) Disclosure Record

Disclosure of patient medical information to a third party is to be documented showing the date, name, and address of the recipient and a general description of the information disclosed (Reference 45 CFR 164.528, Section 456.057(12), Florida Statutes).

(6) Patient Access to Medical Record

A patient receiving treatment from a department facility may inspect and obtain a copy of their patient medical information excluding psychiatric, psychological, or psychotherapeutic notes. Other exceptions exist and legal counsel should be consulted in unfamiliar situations. (Reference Section 456.057(7), Florida Statutes, and 45 CFR 164.524(a)).

(7) Deceased Individual's Medical Record

The patient medical information of a deceased individual is confidential. The authorized representative for disclosure of a deceased individual's medical record is the next of kin or personal representative except for HIV test results which require a personal representative (Reference Sections 395.3025 and 381.0041, Florida Statutes).

(8) De-identified Information

Medical information that has been de-identified in accordance with 45 CFR 164.514 and Section 456.057(7)(a)4., Florida Statutes, and is incapable of being identified to an individual is not confidential and is available for public inspection and copying.

(9) Clinical Laboratory Test Results

Clinical laboratory test results reported by laboratory personnel are to be sent to the licensed practitioner ordering the test. (Reference Section 483.181, Florida Statutes).

f. 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. Patient medical information obtained during this investigation remains confidential and shall not be disclosed without proper authorization except to the licensing authority or otherwise legally waived. (Reference Sections 456.073(2) and 483.181, Florida Statutes).

g. Licensure Applications

All information submitted in an application for health profession and occupation license, except for financial, medical, school transcript information, and examination materials including questions, answers, papers, grades, and grading keys, is subject to public inspection. (Reference Section 456.014, Florida Statutes).

h. Department of Children and Families

Requests from the DCF for disclosure of information on mutual clients will be granted (Reference Section 381.0022, Florida Statutes).

i. Disease Reporting

Medical information received by the department identifying an individual for disease reporting, animal bite, food borne illness or epidemiological research is confidential and only disclosable as necessary to protect public health. Reference Sections 381.0031, Florida Statutes, and 45 CFR 160.203(c).

j. 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 and child care facilities and licensed healthcare providers as specified in department rules (Section 381.003(1)(e), Florida Statutes, Rule 64D-3.011, Florida Administrative Code, and 45 CFR 160.203(c)).

k. Investigations – Child or Adult Abuse and Missing Child

Patient medical information about child or adult abuse or missing children may be disclosed to an investigating law enforcement officer or DCF investigator. (Reference 45 CFR 160.203(c), Sections 39.201 and 415.1034, 937.025(5), Florida Statutes). The Domestic Violence Flow Sheet, form DH 3202, is to be disclosed when patient medical records are subpoenaed. (See section E.1.e.(3) for further information on Subpoenaed Medical Records)

l. Special Needs Shelter (SpNS)

The registry of persons with special needs is confidential, and includes all information gathered concerning a person with special needs in the shelter. The registry information is owned by the local emergency management director and disclosable at his/her direction. Sec. 252.355(5), FS.

m. School Health Records

Records maintained by department personnel assigned to a school health services program (ref sec. 381.0056, FS) for healthcare treatment provided to a student are confidential pursuant to state statute and federal law (Sec. 456.057, FS; 20 USC § 1232g; and 34 CFR 99.31 through 34 CFR 99.33). The local school system is the owner of the records.

n. Vital Statistics

The release of vital statistic information including but not limited to birth, death, and marriage certificates is controlled by Chapter 382 of the Florida Statutes and Chapter 64V-1 of the Florida Administrative Code and not otherwise addressed in this policy.

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

All client and vendor information from the federally sponsored Women, Infants and Children program (WIC) is confidential. This information can be disclosed only to other government agencies providing services to WIC applicants, for child abuse or neglect reporting, in response to subpoenas, court orders, and search warrants after local attorney review, and as authorized by the applicant or vendor. (Reference 7 CFR 246.26(d through g)).

p. Division of Disability Determination

Disclosure of patient medical information 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. (Reference Sections 5 U.S.C. 552 and 42 U.S.C. 1306).

q. Current Law

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 (Reference 45 CFR 164.530(h) (2)).

r. Information Custodian Requirement

The DOH worker disclosing confidential information is responsible to ensure that sufficient authorization has been provided. The information has been reviewed and prepared for disclosure as required, and that no revocation of the requesting document has been received.

s. Legal Review

Before disclosure of any patient medical information in response to a subpoena, court order, or law enforcement demand, legal review is required. Legal review can be accomplished by a request from the local Information Security and Privacy Coordinator for a CHD, CMS clinic, or department division to their assigned legal counsel. The department privacy officer can be contacted in the absence of local legal counsel.

t. 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 DH3204. A business associate agreement maybe required pursuant to DOH Information Security and Privacy Policy 11, DOHP 50-10j-07.

u. Legal Counsel

Legal counsel should be consulted in unfamiliar situations. Exceptions may exist.

2. Requirements for Patient Medical Information Requests

Requests for patient medical information must meet the following requirements (Reference 45 CFR 164.508(c) (1) (i-v)):

- a. A clear description of the information requested.
- b. The identification of the person or entity making the request.
- c. The identity of the DOH 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 personal representative of the individual, a description of the representative's authority to act for the individual 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 (Reference Section 456.057(7)(a), Florida Statutes, and 45 CFR

164.506(c)). Efforts should be made to record any documents actually exchanged between healthcare providers for treatment purposes.

i. Specific authorization will be provided 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. (Reference Sections 381.004, 456.057(7)(a), Florida Statutes, and 45 CFR 164.508(a)(2); Section 397.501(7), Florida Statutes, and 42 CFR Part 2 and 7 CFR 246.26, respectively).

Note: Forms DH 3203 and DH 3204 contain the required elements listed above for requesting and disclosing patient medical information

3. 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.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. This policy has been revised in 2005, 2007, and 2008. This policy was last revised in October 2008 and supersedes previous versions. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Each Department of Health (DOH) division, office, county health department (CHD), Children's Medical Services (CMS) clinic, and the A.G. Holley Hospital must have locally written information security policies and procedures that are consistent with the DOH Information Security and Privacy policy and protocols relating to patients' rights. Patient rights are specified in Florida Statutes and the Health Insurance Portability and Accountability Act (HIPAA).

II. Authority

Not Applicable

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

10/1/07

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

All DOH supervisory employees with access to patient medical records, information security and privacy coordinators, DOH HIPAA Privacy Official, and the DOH contact person.

- C. Competencies
 - 1. Knowledge of applicable federal regulations, state laws, and rules.
 - 2. Knowledge necessary to coordinate the implementation of information privacy policies, protocols, and procedures.
 - 3. Knowledge of policies, protocols, and procedures related to privacy of patient medical information relating to patient rights.

D. Outcomes

1. Each DOH office or program designated as a covered entity shall provide a Notice of Privacy Practices to individuals using the standard DOH form and procedure.
2. Each covered entity shall display in public view a sign advising of the patient's privacy rights.
3. A standard process shall be in place 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. Individuals or their representatives have the right to specific patient rights such as access, amendments, and restrictions of their patient medical information.
5. Patient privacy must be maintained in accordance with Florida Statutes and federal laws.

E. Areas of Responsibility

1. Notice of Privacy Practices
 - a. A Notice of Privacy Practice must be prominently displayed in each covered unit.
 - b. At a client's initial encounter with a DOH covered unit, unless it is an emergency situation, a Notice of Privacy Practices must be given to the client.
 - c. Receipt of the privacy notice shall be documented on the Initiation of Services DH3204, and kept in the client's medical record.
2. Privacy Enforcement/Complaints
 - a. Complaints of inappropriate disclosure must be submitted in writing to the local privacy coordinator, DOH Inspector General, or the Health and Human Services Office of Civil Rights.
 - b. Local client complaints shall be reported to the DOH Inspector General.
 - c. The name, telephone number, and address of the contact officer must be provided.
 - d. The information security/privacy coordinator shall file an incident report if required by DOH Incident Reporting Policy, DOHP 5-6-06.

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

3. Access to Patient Medical Information

a. Access to patient medical information must be provided to a patient upon request or to their personal representative upon written request with proper documentation.

b. Patients or their personal representative may have copies of their patient medical information.

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

d. Access may be denied and no review required if the patient medical information is exempt from access as specified in federal or state law.

e. The patient or personal representative must be notified within 30 days of the decision to permit access or deny access. Division of Disability Determination must respond within 20 days for Social Security Administration determinations. An extension of 30 days may be granted once, if the record is filed off premises.

f. Written notice of the decision to deny access must be given to the patient or personal representative within 30 days. Division of Disability Determination must respond within 20 days for Social Security Administration determinations. The written denial must state the reason for denial and the process to complain to the contact officer.

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

h. If access is denied, the patient has the right to have the action reviewed by a licensed healthcare professional who is designated by the department to act as the reviewing official and who did not participate in the original decision to deny access. The patient must be notified regarding the decision in writing.

4. Amendment to Patient Medical Information

a. The patient or patient representative has the right to request an amendment to their patient medical information.

- b. The request to amend the record must be received in writing and include the reason to support the amendment.
- c. DOH must act within 60 days of the request and may have one 30 day extension if the patient is advised in writing of the cause of the delay.
- d. If the request to amend is granted, DOH must provide the amendment to any previous disclosure recipients identified by the patient.
- e. The request to amend can be denied if:
 - (1) The information was not created by DOH.
 - (2) The information is accurate and complete.
 - (3) The information would not be available for inspection under the right of access.
- f. If the request to amend is denied, the patient must be notified in writing regarding the following:
 - (1) The reason for the denial.
 - (2) A statement of disagreement may be submitted and filed in the record.
 - (3) 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:
 - (a) All documents relating to the request for amendment must be filed in the patient's medical record.
 - (b) If the patient is denied the right to amend the patient medical information, the DOH Privacy Officer must be notified of the action (see to [Appendix B](#), Forms).

5. Accounting of Disclosures/Disclosure Log

- a. Patients have a right to receive an accounting of non-routine disclosures of patient medical information to third parties.
- b. Disclosures to business associates, external and grant audits must be documented.

6. Restrictions of Uses and Disclosures of Patient Medical Information

- a. Patients have the right to place restrictions on uses and disclosures of patient medical information.
- b. Requests for restrictions shall be referred to the Information Security Privacy Coordinator for review and action. DOH is not required to agree to a restriction. If DOH agrees to the restriction, DOH must not disclose the restricted information except in an emergency.

7. Alternate Method of Communications

- a. Patients may authorize alternate methods of communication.
- b. If the alternate method of communication is accepted all communication to the patient must be by the method requested and approved. This must be documented in the medical record and noted in the clinical management system and shared with all programs and departments that could contact the patient. Communication includes billing information.
- c. The patient may change designation of alternate means of communication at anytime.

8. Florida Patient Bill of Rights

Patients' privacy rights are to be respected consistent with providing adequate medical care and efficient facility administration (381.026, F.S.).

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies 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 privacy rule.

II. Authority

See [Appendix C](#), *Summary of Confidentiality statutes Shielding Documents in the Custody of the Department of Health*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

10/1/07

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

All Department of Health (DOH) workers designated to work with the public health programs and activities which include the communicable disease programs, epidemiology, environmental health, bioterrorism and health promotion, and staff assigned the responsibility of disclosing health information.

- E. Competencies
 - 1. Knowledge of applicable federal regulations, state laws, and rules.
 - 2. Knowledge necessary to coordinate the implementation of information privacy policies, protocols, and procedures.
 - 3. Knowledge of policies, protocols, and procedures related to privacy of protected information as it relates to public health activities and investigations.

F. Outcomes

1. Create public health systems and files that are exempt from Protected Health Information.
2. Identify and maintain information related to public health events, disasters and investigations.

G. Areas of Responsibility

1. Individual medical information maintained in a public health disaster, emergency, communicable disease surveillance, or epidemiology investigations are exempt from HIPAA.
2. Notice of Privacy Practices are not required in the following:
 - a. Reportable diseases as specified in Florida Statute.
 - b. Syndromic Surveillance and surveillance of communicable disease or disease outbreaks.
 - c. Epidemiology investigations of communicable disease outbreaks.
 - d. Locating contacts for communicable disease prevention.
 - e. Registries
 - f. Regulatory activities
 - g. Child Abuse Registries
 - h. Environmental Health Program investigations.
 - i. Reporting to Department of Children and Families (DCF) for Missing Child Investigation—statute requirement.
 - j. Community health screening—health fairs, blood pressure (BP) checks.
 - k. Public health student screening.
3. Patient authorization is not required for information to be submitted to the following registries:
 - a. Tuberculosis (TB)
 - b. Sexually Transmitted Diseases (STD)

- c. Human Immunodeficiency Virus (HIV)
- d. Cancer/Tumor
- e. Immunization
- f. Vital statistics
- g. Brain and spinal cord injury
- h. Infant death
- i. Communicable disease reporting
- j. Child death review
- k. Trauma

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Each Department of Health (DOH) contract resulting in the contract provider having access to, or producing (as a result of contract services), confidential department information shall include standard contract language which requires 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.

Each contract provider accessing patient medical information must have a Business Associate Agreement or business associate clause with the department if they are not a covered entity. A Business Associate Agreement is required when the department (as the covered entity) permits a business associate to create, receive, maintain, or transmit electronic patient medical information on the department's behalf.

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.

All department contracts involving information technology shall require that any hardware or software acquired as part of the contract shall either conform to department standards, as determined by the Information Technology Standards Workgroup (ITSW), or is an ITSW approved exception and have been approved through the department's governance process.

II. Authority

See [Appendix B](#), *Standard Third Party Networking Connection Agreement*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

A. Type of Protocol: Administrative

B. Personnel

Directors/Administrators of DOH divisions, offices, county health departments (CHDs), Children's Medical Services (CMS) clinics, and the A.G. Holley Hospital as well as other staff designated responsible for contract management activities, information technology network staff responsible for establishing network connections to outside contractors, and all information technology contracts in the department.

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, procedures, and any amendments. 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. Outcomes

1. The following contract clause is contained in all applicable provider contracts with the department:

*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 medical information. The department reserves the right to review the provider's policies and procedures.*

2. The contract provider has 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 the department.

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

5. Secure network connections will be provided to all outside entities having a third-party network connection to the DOH network. This does not include contractors, vendors, and other outsiders who sign onto or dial into the DOH network via usual DOH network connections.

6. All information technology (IT) contracts will comply with the DOH IT technical standards and the DOH IT governance policies and procedures.

7. Contracts involving the disclosure of patient medical information require a business associate agreement, or business associate clause in a contract attachment. A business associate agreement is not needed if the disclosure is to a covered entity for treatment of an individual, by a group health plan, Health Maintenance Organization, or health insurer.

E. 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 DOH program-specific supplemental protocols for information security and privacy.

b. Assure that the provider has any applicable DOH 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 assure review of provider compliance with confidentiality requirements, including any DOH program-specific supplemental protocols related to confidentiality. The scope, content, and frequency of the review are to be in keeping with any 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 information security and privacy coordinator and systems administrator or designee is responsible to provide technical assistance to the contract manager when needed to support the technical assistance and monitoring activities of the contract manager.
3. Legal staff shall provide review, guidance, and opinions, as needed, to assure legal sufficiency and statewide uniformity for interpretation of confidentiality matters.
4. Headquarters networking staff and security staff 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. The Standard Third Party Networking Connection Request and the Standard Third Party Networking Connection Agreement can be found in Appendix B.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

All information of the Department of Health (DOH) must be retained, archived, and destroyed in accordance with the General Schedule for State Government and the retention requirements of DOH. Data identified as relevant to any pending litigation is to be maintained until the end of the litigation, including any appeal periods. Archiving and disposition procedures must be documented and must be performed in such a way as to ensure that confidentiality and security are maintained. All computer equipment must be sanitized prior to reassignment or disposal to ensure that the confidentiality of department data is maintained.

II. Authority

See [Appendix C](#), *Summary of Confidentiality statutes Shielding Documents in the Custody of the Department of Health*.

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel
 - 1. All DOH workers, including contractors and volunteers.
 - 2. Bureau of General Services
 - 3. Records Management Liaison Officer (RMLO)
 - 4. Division of Information Technology
 - 5. Department of Health Systems Administrators

C. Competencies

1. Knowledge of federal and state statutes, rules, and regulations pertaining to records management, asset management, exemptions from disclosure, and requirements for maintaining confidentiality of information.
2. Knowledge of established departmental policies and protocols related to records management, asset management, security, and privacy of information.

D. Outcomes

1. All department data will be properly archived, retained, and disposed in accordance with applicable state and federal law and statutes.
2. Confidential department data shall not be disclosed to unauthorized persons.

E. Areas of Responsibility

1. The Bureau of General Services is responsible for publishing retention schedules for all department data, reference the Records Management policy; management of the department's state-owned property, reference Asset Management policy and procedure; the authorization for disposal of all state-owned computer hardware and the electronic media contained therein; and for publishing protocols and procedures for asset management of state-owned property and records management.
2. The director, bureau chief, or administrator for the respective office shall designate a local RMLO. The local RMLO is the person assigned the responsibility of record management and who is responsible for quality control of records in the assigned office, division, laboratory, clinic, or CHD within DOH.
3. When authorized by the applicable retention schedule, confidential information, regardless of media type, must be destroyed in appropriate manner.
4. The Division of Information Technology is responsible for publishing protocols and procedures for sanitization of all DOH-owned computer equipment prior to reassignment or disposal.
5. Local DOH systems administrators at the location responsible for the computer equipment will ensure that data is backed up before moving the equipment and performing the sanitization procedures.

VII. Procedure

1. Sanitizing Computer Equipment

Sanitization is the removal of data from storage media so that, for all practical purposes, the data cannot be retrieved or utilized. The process of sanitization is required whenever media is transferred from one individual to another, when equipment is declared surplus, and when organizations dispose of media. When computer equipment is planned for reassignment or surplus, the local system administrator or designee is responsible for sanitizing the equipment by performing the following:

- a. Ensuring that notification and documentation of the reassignment or surplus have been given to persons responsible for updating asset management records so that the appropriate updates can be made in accordance with the Department of Health's Asset Management policy and procedure.
- b. Sanitizing the equipment using software that ensures no data remains. (See the methods and tools recommended by the National Institute of Standards and Technology).
- c. Deletion of files is not an approved method of sanitization.
- d. Approved sanitization methods are:
 1. Overwriting is the utilization of software to write over, or cover, data on computer media so that the data is no longer retrievable.
 2. Degaussing is a method to erase data from magnetic media. It may be utilized when overwriting of the media is not possible.
 3. Destruction of the computer media is a method of sanitizing that physically damages the media. It may be utilized for equipment planned for surplus when overwriting or degaussing of media is not possible.

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in

August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Risks to data and information technology resources must be managed. Directors/Administrators of Department of Health (DOH) divisions, offices, county health departments (CHDs), Children's Medical Services (CMS) clinics, and the A. G. Holley Hospital must conduct an annual risk analysis, using the current DOH Information Security and Privacy Risk Assessment form. Documentation of the risk analysis and any correction action plans must be accessible to management and filed with the DOH Information Security Manager. Documentation of the risk assessment and corrective action plan is confidential.

II. Authority

Not Applicable

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

A. Type of Protocol: Administrative

B. Personnel

Directors/Administrators of DOH divisions, offices, CHDs, CMS area offices, the A. G. Holley Hospital, 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 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.
5. Knowledge of policies, protocols, and procedures related to the privacy and the security of information.

D. Outcomes

1. A risk analysis is conducted at least annually and an onsite risk analysis is conducted every three years.
2. In coordination with the state Office of Information Security (OIS), the DOH Division of Information Technology shall conduct a comprehensive risk analysis of critical information resources and notify OIS upon completion.
3. Documentation of security and privacy corrective action plans is confidential and not subject to public disclosure.
4. Corrective action plans are accessible to departmental management.
5. Corrective action steps will be documented and monitored through final implementation by the appropriate agency manager.
6. Corrective action plans must identify the relative risk of the corrective action required. Implementation schedules must address those items with a high relative risk first.
7. Operating procedures are updated, where appropriate, to reflect changes as a result of the risk analysis and corrective action plan.

E. Areas of Responsibility

1. A copy of the completed DOH Security and Privacy Risk Analysis must include a corrective action plan.
2. Corrective action plans are developed in a manner, which clearly identifies the finding, the steps required to correct the situation, the expected date of completion, and the individual(s) responsible for implementing and monitoring the action item.
3. Corrective action plans must be discussed with the individual(s) who have the responsibility or authority to make recommendations for improvement, implement corrective actions, and monitor corrective action steps.

4. Operating procedures are updated, where appropriate, to reflect changes as a result of the corrective action plan.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

Each Department of Health (DOH) division, office, county health department (CHD), Children's Medical Services (CMS) clinic, and the A. G. Holley Hospital must develop and adopt a written, cost-effective contingency plan to provide essential functions and recover critical information in the event of any disaster, natural or intentional. Documentation shall be incorporated into the local Continuity of Operations Plans (COOP) and Continuity Operations for Information Technology Plans (COOP-IT), which are required by state and federal law. The contingency planning process should identify critical functions; document practices for the back up, storage and retrieval of electronically stored information; and annually test the plans.

II. Authority

- A. Public Law 104-191
- B. 45 Code of Federal Regulations (C.F.R.), Parts 160 and 164
- C. Florida Statutes (F.S.) section 282.318
- D. Florida Administrative Code (F.A.C) 60DD

III. Supportive Data:

Federal and state laws, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

All DOH divisions, offices, CHDs, CMS area offices, and the A.G. Holley Hospital as well as other staff designated with the responsibility of the following:

1. Contingency planning for the continuity of business operations and disaster recovery of the information technology function.

2. Providing essential information systems must back up information to ensure continued availability in the event of a disaster (major or minor) while also protecting confidentiality and data integrity of department information.

C. Competencies

1. Knowledge of federal and state statutes, rules, and regulations pertaining to security, contingency planning, business continuity planning, and disaster recovery planning.

2. Knowledge of established departmental policies and protocols related to security, contingency planning, business continuity planning, and disaster recovery planning.

3. Knowledge of information technology security and practices.

D. 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

E. Areas of Responsibility

1. Disaster Recovery Planning

All functions determined by management to be essential to the department's mission shall have a written COOP that will provide for the prompt and effective continuation of critical state functions in the event of a disaster, natural or manmade. This is a requirement of state and federal law.

a. Management must prepare, periodically update, and regularly test a business recovery plan, known as the COOP. This plan must specify how alternative facilities such as offices, furniture, telephones, and copies, etc. will be provided so workers can continue mission-critical operations in the event of either an emergency or a disaster.

b. Management must prepare, periodically update, and, at a minimum, annually test a disaster recovery plan that will allow all critical information technology and communication systems to be available in the event of a major loss such as a hurricane, tornado, or flood. This plan is also known as the COOP-IT Plan.

c. A standard process for developing and maintaining both business contingency plans and computer contingency plans must be documented and maintained by headquarters personnel. The department's COOP coordinator will be responsible for overall development and coordination of business continuity, or COOP, plans. The Division of Information Technology will be responsible for determining disaster recovery, or COOP-IT, planning and plan documentation standards, as well as for coordinating the headquarters disaster recovery planning and testing.

d. Local information technology (IT) disaster recovery coordinators, with the assistance of regional disaster preparedness consultants, local Information Security and Privacy Coordinators, and other local IT staff, are responsible for coordinating the local disaster recovery planning and testing functions, using the planning process and plan documentation standards established by headquarters IT. 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) Assurances 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.
- e. Information custodians must play a major role in the development and implementation of the department's contingency planning and testing process, which includes both the business continuity and disaster recovery functions.
- f. Information technology recovery plans must be tested at least annually to assure that plan documentation is kept up-to-date and that the plans continue to be relevant and effective. Each test must be followed by any necessary documentation updates and a brief written report to management and headquarters IT detailing the results of the test and remedial actions that will be taken.
2. Data Backup
- a. All DOH personal computer users are responsible for backing up the information on their computers, either by backing up to the shared drive or making individual backup copies. If they choose to make individual backup copies on an electronic media, such as a floppy disk or CD, they are also responsible for safeguarding the backup copies.
 - b. DOH local systems administrators are responsible for making periodic backups of servers and other multi-user systems, for cataloging and safeguarding the backups, and for transporting off-site backups.
 - c. Local Information custodians must define which information and which machines are to be backed-up, the frequency of back-up, and the method of back-up based on the following guidelines:
 - (1) If the system supports more than one individual and contains data that is critical to the day-to-day DOH operations, then back up is required weekly.
 - (2) If the system is used to support job-related functions and contains key data critical to the day-to-day operation of that job, then back up is required weekly.
 - (3) 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, then back up is at the discretion of the individual user.

- d. Nothing in the time frames for periodic back up restricts the generation of more frequent back-ups. For example, if hurricane warnings have been announced or there is a reason to suspect the integrity or reliability of the system involved, an immediate back-up is advisable.
- e. The department requires the use of at least two (2) sets of back-up 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.
- f. All back-up computer media (magnetic tapes, floppy disks, optical disks, etc.) stored off-site must be physically protected against unauthorized access and other common mishaps like water or fire damage.
- g. If a third-party vendor is contracted to perform offsite storage, the following conditions should be met:
- (1) The backup media will need to be stored in a physically secure fashion to protect them from common mishaps like water damage and fire damage.
 - (2) The media must either be stored in an encrypted format or in their own secured box inaccessible to unauthorized workers.
 - (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 medical information (PMI) 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.
- h. All computers containing electronic PMI should be backed up prior to movement of equipment, per Health Insurance Portability and Accountability (HIPAA) requirements.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors
Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies is responsible for this policy.

I. Policy

The Department of Health (DOH) information technology (IT) resources are critical to the DOH mission; the confidentiality, integrity, and availability of those resources must be protected.

DOH information technology resources must be managed and operated effectively to ensure a reliable IT infrastructure.

Measures must be taken to ensure that department networks remain available and secure. Only approved hardware and software is permitted. IT security processes, devices, and software will be implemented to protect IT resources. Changes to the production environment must be managed. IT workers must be competent and responsible. Access to data and information systems must be controlled to ensure only authorized individuals are allowed access to information and that access should be granted upon a “need-to-know” basis. Software applications must be designed and configured with proper security controls.

Deviation from this policy requires a written approval for an exception from the DOH Chief Information Officer (CIO).

II. Authority

See [Appendix C](#), *Summary of Confidentiality Statutes Shielding Documents in the Custody of the Department of Health*.

III. Supportive Data

- A. Federal and state Law, rules, and regulations referenced in [Appendix C](#).

IV. Signature Block with Effective Date

Signature on file

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

10/1/07

Date

V. Definitions

Referenced in [Appendix A](#), *Definitions and Glossary*.

VI. Protocol

- A. Type of Protocol: Administrative
- B. Personnel

Directors/Administrators of DOH divisions, offices, CHDs, CMS area offices, the A. G. Holley Hospital, system administrators, IT workers, and other staff designated

responsible for operating, developing, administering, or managing DOH IT resources and staff.

C. Competencies

1. Knowledge of established departmental policies and protocols related to security and privacy of information.
2. Knowledge of federal and state statutes, rules, and regulations pertaining to security and privacy.
3. Knowledge of information technology resource security requirements and best practices.
4. Knowledge and skills to apply and maintain technical information security policies, procedures, and practices.

D. Outcomes

1. Information security policies, procedures, and practices which incorporate all elements of required technology standards and practices.
2. IT infrastructure and IT workers are managed appropriately and effectively.
3. Written local operating procedures for implementation of IT issues.
4. Integrity of department resources is maintained and IT resources are protected against unauthorized access, alteration, disclosure, or destruction.
5. Confidentiality is maintained.
6. Availability of IT resources is maintained.
7. Appropriate security measures are implemented to mitigate increased security risks presented by using wireless technologies.
8. 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.

E. Areas of Responsibility

1. Infrastructure Management
 - a. Information Technology Resources

- (1) Only DOH-managed information technology resources will connect to the DOH network. Exceptions must be granted in writing by the Information Security Manager (ISM) and CIO.
 - (2) Access to and use of DOH IT resources is reserved for DOH-authorized users and purposes.
 - (3) The DOH CIO or delegate has final authority regarding access to the DOH network and IT resources.
 - (4) The Security Administration Team will monitor for unauthorized information technology resources connected to the DOH network.
 - (5) The Division of IT will implement procedures to track agency information technology resources and associated owners and custodians.
- b. Information Technology Workers
- (1) IT positions are positions of special trust.
 - (2) The agency will conduct background investigations for workers in positions of special trust as set forth in sections 110.1127, Florida Statutes.
 - (3) The Division of IT will document minimum qualifications relative to training and experience for IT workers.
 - (4) The department must provide on-going training for information technology workers to ensure competency in both technical and security aspects of their positions.
 - (5) IT workers will be granted access to agency information technology resources based on the principles of "least privilege" and "need to know."
 - (6) The department will implement controls to ensure access to information technology infrastructure resources is restricted to authorized users and uses.
 - (7) The department will ensure separation of duties, so no individual has the ability to control an entire process.
- c. Information Technology Hardware and Software Standards
- (1) The Information Technology Standards Workgroup (ITSW) will specify standard software and hardware for use at DOH.

(2) The ITSW will approve certain non-standard software and hardware for use in specific circumstances at DOH.

(3) The ITSW will coordinate risk assessment/feasibility studies prior to approving a new technology (e.g., voice over IP) at DOH.

(4) The ITSW will maintain lists of approved software and hardware.

(5) The Security Administration Team will specify standard configurations used to harden information technology resources.

d. Network and Perimeter Security

(1) The Security Administration Team will establish DOH configuration standards for DOH firewalls.

(2) The Security Administration Team will perform initial configuration of DOH personal firewalls used for employee remote access.

(3) The Division of IT will ensure network perimeter security measures are in place to prevent unauthorized connections to agency information technology resources.

(4) Unauthorized peer-to-peer traffic is prohibited.

e. Administration of Information Technology Resources

(1) Administration of hardware, software, or applications performed over a network will be encrypted (where technology permits).

(2) System administrators will implement administrative, technical, and physical controls to protect information technology infrastructure resources.

(3) The Division of IT will administer all Internet-facing DOH servers (i.e., Demilitarized Zone – DMZ – servers).

(4) IT resources will be configured to lock out a user ID after a maximum number of unsuccessful login attempts.

(5) User password management shall only be performed in accordance with approved user password management

procedures and utilizing only approved user password management tools (i.e., P-Synch).

f. Resource Monitoring

(1) The Security Administration Team will implement procedures to review records of information system activity, such as system audit and security logs.

(2) The Security Administration Team and Root Administrator staff will have the capability to monitor all devices on the DOH network.

(3) The Security Administration Team will be granted access to review audit logs containing account activity details.

g. IT Change and Release Management

(1) The development infrastructure, test infrastructure, and production infrastructure will be physically or logically separated.

(2) The Change Management process will be used for new systems and applications; modifications to existing systems and applications; and deletion of systems and applications.

(3) The Change Management process will include a verification process ensuring compliance with agency standards and hardening configurations including but not limited to vulnerability assessments for DOH 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.

h. Patch Management

(1) The Division of IT will implement a patch management process for information technology resources.

(2) The Security Administration Team will coordinate patch management process for security patches of DOH enterprise software.

(3) System administrators will ensure approved patches are applied within the designated timeframes.

- (4) System administrators will ensure that patches for non-standard (ITSW approved exceptions) IT resources are tested and applied when appropriate.
- i. Malware Control
 - (1) All state computer systems must have current and up-to-date DOH standard anti-malware software.
 - (2) System administrators will ensure anti-malware software is maintained on agency information technology resources.
 - (3) System administrators will ensure malware-infected computer systems are removed from the network until they are cleaned.
 - j. Service Accounts
 - (1) System administrators will ensure service accounts are maintained in a manner that protects information technology resources.
 - (2) Service accounts may be exempted from password expiration.
 - (3) Service accounts must not be used for interactive sessions.
 - k. Administrative Accounts
 - (1) The Division of IT will establish procedures to ensure administrative rights are restricted to IT workers who are authorized based on an IT position title, documented job duties and responsibilities requiring administrative rights, and who have received appropriate technical training.
 - (2) The Division of IT will establish procedures to ensure accounts with administrative rights are created, maintained, monitored and removed in a manner that protects IT resources.
 - (3) The CIO or delegate will authorize each administrative account prior to creation and will review and reauthorize all administrative accounts annually.

(4) Administrative account activities will be traceable to an individual.

I. Access Security—Termination of Access Rights

A system administrator will deactivate a worker's account for the following reasons: termination of employment or contact; nonuse of account for 60 consecutive days, notification of security violation (by management direction).

m. Remote Network Access

(1) Requests for remote access to the DOH network will be made in writing to the Division of IT.

(2) Remote access to the DOH network is for use by approved DOH workers for business use only.

(3) Remote access client connections may not be shared.

(4) Remote access client requests will be signed by the worker's supervisor (attesting that he/she has reviewed with the requestor the applicable DOH policies including security/privacy, computer use, overtime and compensatory time, and telecommuting), director or administrator of the unit (accepting associated financial obligations), and the local system administrator (attesting that all information on the form is accurate).

(5) Remote access requests will be reviewed for final approval by the CIO or designee.

(6) An non-DOH entity may be granted remote access to specific DOH information technology resources by the CIO or designee.

(7) The Security Administration Team will implement procedures to obtain required information and agreements from non-DOH entities that require remote access to the DOH network (including but not limited to Third party Network Connection Request and Third Party Networking Connection Agreement).

n. Wireless Networks

(1) Wireless technologies will not serve as substitutes for wired networks.

- (2) Only ITSW-approved wireless devices, services, and technologies will be used when connecting to the DOH network.
 - (3) The Security Administration Team will manage all department wireless access points.
 - (4) Agency wireless access points shall be tracked by the department.
 - (5) The department shall monitor for unauthorized access points.
 - (6) Unauthorized access points connected to the DOH network must be removed immediately.
 - (7) System administrators will submit a site survey to the Bureau of Strategic Information Technologies prior to implementation of a wireless network.
 - (8) Wireless transmission of DOH data must be encrypted.
 - (9) Department wireless devices must be configured and maintained according to agency standards
 - (10) Wireless access into the DOH network must require user-authentication.
 - (11) Clients connected to the DOH network must not be simultaneously connected to any other network.
 - (12) DOH equipment may only be connected wirelessly to DOH approved and authorized wireless networks (IEEE 802.11).
- o. Software Application Security Requirements
- (1) The Bureau of Application Development will develop procedures to ensure application security is addressed throughout the application procurement process and/or application development lifecycle.
 - (2) Any third-party application that requires DOH data be stored on non-DOH servers must be approved for use by the CIO 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 agency information technology resources.

(6) A final application security review must be approved by the application owner, Information Security Manager (ISM) and the CIO, or their respective designees, before an application is placed into production.

(7) 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.

(8) Application security documentation shall be maintained by the department and be available to the ISM.

p. 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) The ISM or other authorized workers will be granted access to review audit logs containing accountability details.

VII. Procedure

Applicable standard operating procedures (SOPs).

VIII. Distribution List

Chief of Staff
Deputies
Executive Office Directors

Division Directors
Bureau Chiefs
County Health Department Directors/Administrators
Children's Medical Services Medical Directors
Children's Medical Services Nursing Directors
Children's Program Administrators
Web Managers
AG Holley Hospital

IX. History Notes

Original effective date of the Information Security policy was signed November 1999. The April 2005 Information Security and Privacy policy supersedes the original. This policy was revised in August 2007. The Division of Information Technology, Bureau of Strategic Information Technologies 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—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 agency performs or assists in the performance of a function or activity involving the use or disclosure of protected medical information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by the HIPAA privacy rule.

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

Comprehensive Risk Analysis—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.

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—Ensuring that information is accessible only to those authorized to have access. The state that exists when confidential information is held in confidence and available only to a limited set of authorized individuals pursuant to applicable law. Confidentiality is the security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads.

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, backup 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 clinic and the A. G. Holley Hospital will have a COOP plan.

Continuity of Operations Plan for Information Technology (COOP-IT)—This is 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 agency management to be essential to the agency’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 condition existing when the data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Data Security—The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized.

Department of Health (Department)—All Department of Health divisions, offices, county health departments, Children’s Medical Services clinics, and the A.G. Holley Hospital.

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 agency 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 ciphertext) 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 workers, contractors, vendors, third parties, and volunteers in a part-time or fulltime capacity.

Federal Information Processing Standard Publication Nr (FIPS PUB NR)—A federal standard issued by the National Institute of Science and Technology (formerly the National Bureau of Standards).

Governance—The formal structure established within the Department of Health to facilitate information technology planning, policy and procedure development, prioritization, and project monitoring (see DOHP 50-3-03 Information Technology Governance Policy).

HIPAA Privacy Compliant Officer—The department’s Inspector General functions as the Agency Privacy Compliant Officer and serves as a focal point for all complaints of privacy violations.

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.

HIPAA Reviewing Officer (physician)—A licensed health care professional who has been assigned the responsibility of Reviewing Official for each of the covered units 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.

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.

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)

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 or Information Resource Custodian—Agency workers 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 Information Resource Owner—Agency managers who are responsible for specifying the security properties associated with the information their organization possesses and are responsible for the integrity and accuracy of that information. This includes what categories of users are allowed to read and write various items and what the operational impact of violations of policy would be.

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 paragraph 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 agency's information resource security program and plans in accordance with Section 282.318(2)(a)1, F.S., and the agency'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 clinic, 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 agency's mission and establish controls to assure adequate security for all information processed, transmitted or stored in agency automated information systems, e.g., Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

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 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 50-9-04 Information Technology Acquisition Policy).

Information User or Information Resource User—See End User

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.

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.

Minimum Necessary Rule—Criteria designed to limit the request for protected medical information to the information reasonably necessary to accomplish the purpose for which the request is made.

Mobile Computing Device—A laptop, PDA, 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, and cell phones or tape drives that may be easily attached to and detached from computing devices.

National Institute of Standards and Technology (NIST)—Founded in 1901 and formerly known as the National Bureau of Standards, 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—The necessity for access to, knowledge of, or possession of specific information that is required to carry out official duties.

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. 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, Section 456.057, 395.3025, 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).

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

Protected medical 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 health 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 Tuberculosis (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 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 device 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 Comprehensive Risk Analysis.

Risk Assessment—See Comprehensive Risk Analysis.

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 the 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 and authentication token) is a small hardware device that the owner carries to authorize access to a network service.

Security Vulnerability Assessment—A 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. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

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.

Streaming media—Sound (audio) and pictures (video) that are transmitted on the Internet in a streaming or continuous fashion, using data packets. The most effective reception of streaming media requires some form of broadband technology such as cable modem or DSL.

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.

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

Acceptable Use and Confidentiality Agreement

http://dohiws/Divisions/IRM/Policies/Security/DH_1120_AcceptableUseandConfidentialityAgreement.pdf

Authorization for Non-Routine Disclosure of Patient Medical Information

http://dohiws/Divisions/IRM/Policies/Security/DH_3203_081002_0735h.doc

Cooperative Agreement between the DOH and Colleges and Universities

http://dohiws/Divisions/IRM/Policies/Security/AGREEMENT_BETWEEN.pdf

Incident Reporting Policy, Forms and Instructions

http://dohiws.doh.state.fl.us/Divisions/Insp_General/IncidentReports.htm

Initiation of Services

http://dohiws/Divisions/IRM/Policies/Security/DH_3204_081002_0735h.doc

Instructions for Initiation of Services

http://dohiws/Divisions/IRM/Policies/Security/DH_3204_Instructions_081002_0735h.doc

Standard Third Party Networking Connection Agreement

http://dohiws/Divisions/IRM/Policies/Security/DH_6007_StandardThirdPartyNetworkingConnectionAgreement.pdf

Third Party Network Connection Request

http://dohiws/Divisions/IRM/Policies/Security/DH_6008_ThirdPartyNetworkingRequestForm.pdf

Transmittal Letter Suggested Language

http://dohiws/Divisions/IRM/Policies/Security/Transmittal_letter_sugg_language_2008.doc

**SUMMARY OF CONFIDENTIALITY STATUTES
SHIELDING DOCUMENTS IN THE CUSTODY OF THE
DEPARTMENT OF HEALTH
(Updated February 2004)**

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
383.410	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	Unemployment Comp. – 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	Adverse incident report
456.082	Criminal penalty for breach of confidentiality
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)&.0615(2)(c)	Pesticide registration & “Review Council”
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)	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

VII. SUMMARY OF DOH CONFIDENTIALTY RULES

A. 64C-7.006	B. Metabolic and heredity disorder screening records
C. 64C-7.010	Infant risk screening records (prenatal & postnatal)
D. 64D-2.003	HIV
E. 64D-2.004	HIV
F. 64D-2.006	HIV
G. 64D-3.016 & 3.017	STD reports including HIV and AIDS
H. 64D-3.018	Partner notification
I. 64F-6.005	School health records – students
J. 64F-7.004	Family planning–notification of abnormal lab results
K. 64F-10.008	Primary care projects – client records
L. 64F-12.021	Fla. Drug Device & Cosmetic Act – trade secrets

I. Virus Protection: Virus Indicators. Some of the ways in which viruses propagate so quickly include:

- A. Sharing infected mobile storage devices between users.
- B. Downloading programs from public electronic bulletin boards or other unreliable sources.
- C. E-mail attachments.
- D. Using infected demonstration, system, or software diskettes.

II. Virus Symptoms: There are various kinds of symptoms that some virus authors have written into their programs such as messages, music, and graphical displays. However, the main indications include:

- A. 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.

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 Department of Health workers in order to minimize the risk of introducing viruses and other malicious software, to ensure timely detection of viral infections, to eliminate viral infections from the inventory of microcomputers, and to minimize the risk from malicious programs to larger or network systems.

- A. Check all new software for infection before running it for the first time. It is advisable to use multiple anti-virus programs recommended by the Information Technology Standards Workgroup. **No single anti-virus software is able to detect all viruses.** Certain other software programs may be appropriate pending the review and approval of the Information Technology Standards Workgroup.
- 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 public electronic bulletin boards. When it is necessary to download from an authorized source, download to a diskette and use virus scanning software to test for viruses before copying files to a hard disk. Never download software to a network server.
- D. Do not use diskettes from home systems or other external sources that have not been scanned for viruses. Do not copy copyrighted software or share software with other members of the workforce. Externally supplied diskettes may not be used on any DOH workstation or Local Area Network (LAN) server unless these diskettes have first

been checked for viruses and received a decal indicating that no viruses were found and the date of the virus scan.

E. Protect system files, critical data files, and applications by making backup copies and storing them on write-protected diskettes or the network.

F. A system administrator should have a backup copy of every software program each time it is modified in accordance with established software development procedures and controls. The system administrator should also periodically scan the servers for viruses and maintain a scan log with information such as the date of the scan, and results of the scan.

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.

E. **NOTE:** 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. 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 a write-protected diskette containing the anti-virus software.
2. Scan the hard drive (memory, boot sector, and all files) for viruses.
3. Identify any viruses found, by name.
4. Clean any specific viruses found.

5. Rescan the hard drive.
 6. Scan and clean all diskettes.
 7. Attempt to determine source of infection for tracking purposes.
 8. Determine any other infections that may have occurred as a result of the infection.
 9. Report results to management.
 10. Restore any lost software from its original write-protected media.
- H. If possible, restore any lost backup data from virus scanned media.
- I. Log type of virus and measures taken to eradicate virus.
- J. A security incident report must be completed on all confirmed virus infections and reported the Department of Health Security Coordinator for tracking and auditing purposes.

Password Construction**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.

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.

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.

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."

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.

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.

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.

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.

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 Section 119.07 F.S. Some records for deaths in Florida may be found as far back as 1877.

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.

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.

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.

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.

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.

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.

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.