



FDOH Information and Privacy Awareness Training Learner Course Guide

DOH Mandatory Training FY 2013-2014

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



Table of Contents

SECTION	SLIDE NUMBER - TITLE	PAGE
1	Slide 1 – Welcome Slide	1
	Slide 2 – How to Use Navigation	1
	Slide 3 – Section 1 Objectives	2
	Slide 4 – Section 1 Objectives	2
	Slide 5 – Federal and State Policies and Regulations	3
	Slide 6 – What is HIPAA?	3
	Slide 7 – What are the specific HIPAA rules?	4
	Slide 8 – What are the specific HIPAA rules?	4
	Slide 9 – Federal and State Policies and Regulations	5
	Slide 10 – Federal and State Policies and Regulations	5
	Slide 11 – Florida Public Records Act, Chapter 119.07, F.S.	6
	Slide 12 – Florida Public Records Act	6
	Slide 13 – Enterprise Security of Data and Information Technology Act, Chapter 282.318, F.S.	7
	Slide 14 – Enterprise Security of Data and Information Technology Act	7





SECTION	SLIDE NUMBER – TITLE	PAGE
1	Slide 15 – Enterprise Security of Data and Information Technology Act	8
	Slide 16 – Florida Computer Crimes Act, Chapter 815 F.S.	8
	Slide 17 – DOH Information Security and Privacy Policy	9
	Slide 18 – DOH Information Security and Privacy	9
	Slide 19 – Information Security and Privacy Section	10
	Slide 20 – Data Classification Section	10
	Slide 21 – Designation of Security and Privacy Personnel Section	11
	Slide 22 – Designation of Security and Privacy Personnel Section	11
	Slide 23 – Designation of Security and Privacy Personnel Section	12
	Slide 24 – End Slide Section 1	12





Table of Contents

SECTION	SLIDE NUMBER - TITLE	PAGE
2	Slide 1 – Welcome Slide	13
	Slide 2 – How to Use Navigation	13
	Slide 3 – Section 2 Objectives	14
	Slide 4 – DOH Information Security and Privacy Policy	14
	Slide 5 – Acceptable Use and Confidentiality Agreement Section	15
	Slide 6 – Acceptable Use and Confidentiality Agreement Section	15
	Slide 7 – Acceptable Use and Confidentiality Agreement Section	16
	Slide 8 – Acceptable Use & Confidentiality Agreement Section	16
	Slide 9 – Acceptable Use & Confidentiality Agreement Section	17
	Slide 10 – Acceptable Use & Confidentiality Agreement Section	17
	Slide 11 – Acceptable Use & Confidentiality Agreement Section	18
	Slide 12 – Acceptable Use & Confidentiality Agreement Section	18
	Slide 13 – Security and Privacy Awareness Training Section	19
	Slide 14 – Secured Areas and Physical Security Procedures Section	19





SECTION	SLIDE NUMBER - TITLE	PAGE
2	Slide 15 – Secured Areas & Physical Security Procedures Section	20
	Slide 16 – Secured Areas & Physical Security Procedures Section	20
	Slide 17 – DOH Information Security and Privacy Policy	21
	Slide 18 – Confidential Information Section	21
	Slide 19 – Confidential Information Section	22
	Slide 20 – Confidential Information Section	22
	Slide 21 – Confidential Information Section	23
	Slide 22 – Confidential Information Section	23
	Slide 23 – Confidential Information Section	24
	Slide 24 – Confidential Information Section	24
	Slide 25 – Disclosure of Confidential Information Section	25
	Slide 26 – Disclosure of Confidential Information Section	25
	Slide 27 – Disclosure of Confidential Information Section	26
	Slide 28 – End Slide Section 2	27





Table of Contents

SECTION	SLIDE NUMBER - TITLE	PAGE
3	Slide 1 – Welcome Slide	28
	Slide 2 – How to Use Navigation	28
	Slide 3 – Section 3 Objectives	29
	Slide 4 – DOH Information Security and Privacy Policy	29
	Slide 5 – Patient Privacy Rights Section	30
	Slide 6 – Patient Privacy Rights Section	30
	Slide 7 – Patient Privacy Rights Section	31
	Slide 8 – Patient Privacy Rights Section	31
	Slide 9 – Patient Privacy Rights Section	32
	Slide 10 – Patient Privacy Rights Section	32
	Slide 11 – Patient Privacy Rights Section	33
	Slide 12 – Public Health HIPAA Exemptions Section	33
	Slide 13 – Public Health HIPAA Exemptions Section	34
	Slide 14 – Public Health HIPAA Exemptions Section	34



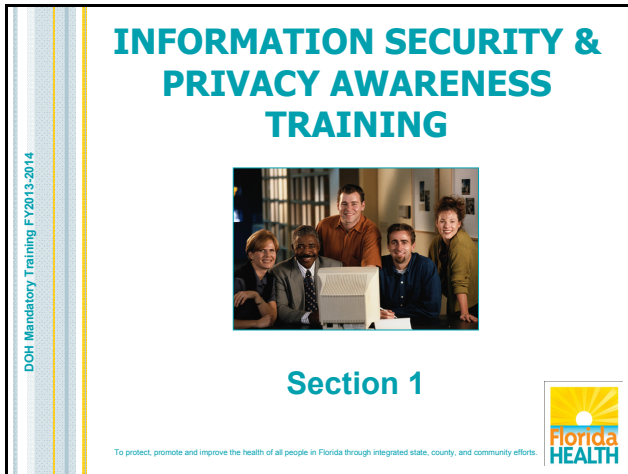


SECTION	SLIDE NUMBER - TITLE	PAGE
3	Slide 15 – Public Health HIPAA Exemptions Section	35
	Slide 16 – Contract Providers and Business Associates Section	35
	Slide 17 – DOH Information Security and Privacy Policy	36
	Slide 18 – Retention, Archiving and Disposition of Records Section	36
	Slide 19 – Retention, Archiving and Disposition of Records Section	37
	Slide 20 – Risk Analysis Section	37
	Slide 21 – Contingency Planning Section	38
	Slide 22 – Contingency Planning Section: Continuity of Operations for Information Technology Plans – COOP-IT Plan	38
	Slide 23 – Information Resource Management Security Section	39
	Slide 24 – Have Questions?	39
	Slide 25 – End Slide	40



Section 1

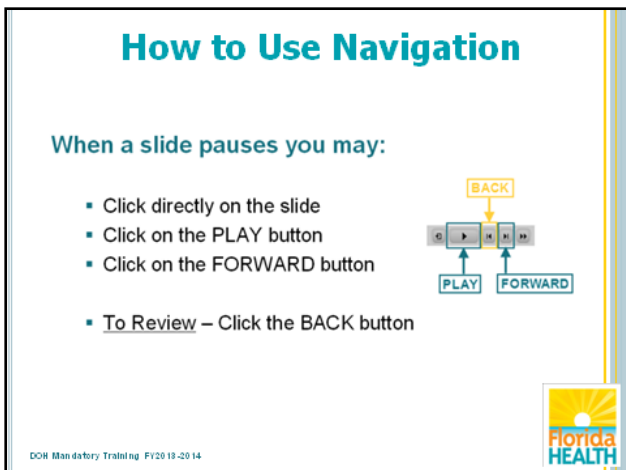
Slide 1 – Welcome Slide



Welcome to the Florida Department of Health's Information Security and Privacy Awareness Training - Section 1.

In this section, we will explain the importance of information security and privacy awareness in order for you to be aware of the rules and regulations and to act accordingly based on these rules.

Slide 2 – How to Use Navigation



In order to make your training experience as easy as possible during the course of this self-paced DOH Mandatory Training course, we are providing these navigation instructions.

When a slide pauses you can do one of three things to advance the presentation:

You may click directly on the slide with your cursor
You may click on the PLAY button on the bottom left of the screen
or
You may click on the FORWARD button, also located on the bottom left of the screen.

If you need to review a previous slide you may click the BACK button on the bottom left of the screen.


Please keep these instructions in mind as you proceed with this training. You will need to advance the slide now.

Slide 3 – Section 1 Objectives

Section 1 Objectives

Recognize HIPAA rules, the federal & state rules, & regulations related to information security & privacy:

1. Public Records Act 119.07, F.S.
2. Enterprise Security of Data & Information Technology Act Chapter 282.318, F.S.
3. Florida Computer Crimes Act Chapter 815, F.S.



DOH Mandatory Training FY2013-2014

Upon completion of this section, you will be able to recognize HIPAA rules, the federal and state rules, and regulations related to information security and privacy, such as


1. The Public Records Act, Chapter 119.07, Florida Statute, and
2. The Enterprise Security of Data and Information Technology Act, Chapter 282.318, Florida Statute, and
3. The Florida Computer Crimes Act, Chapter 815, Florida Statute

Slide 4 – Section 1 Objectives

Section 1 Objectives

Identify DOH Information Security & Privacy Policy Sections:

1. Information Security & Privacy
2. Data Classification
3. Designation of Key Security & Privacy Personnel



DOH Mandatory Training FY2013-2014


You will also be able to identify the following sections of the Department of Health's Information Security and Privacy policy:

1. Information Security and Privacy
2. Data Classification and
3. Designation of Key Security and Privacy Personnel




Slide 5 – Federal and State Policies and Regulations

Federal & State Policies & Regulations



- What is HIPAA?
- What are the specific HIPAA rules?
- What are the Federal & State Information Security & Privacy policy statutes & regulations?



DOH Mandatory Training FY2013-2014

This first section will give you a general idea about the Federal and State, Information Security and Privacy policy, statutes and regulations. We will answer these three questions:


- What is HIPAA?
- What are the specific HIPAA rules? and
- What are the Federal and State Information Security and Privacy policy statutes and regulations?

Slide 6 – What is HIPAA?

What is HIPAA?

Health Insurance Portability & Accountability Act, Public Law 104-191

- Establishes standards to improve the efficiency & effectiveness of the country's health care system
- Applies such practices to all health care providers in the United States
- Strengthens penalties for violations



DOH Mandatory Training FY2013-2014

HIPAA is the acronym for the Health Insurance Portability and Accountability Act. It establishes standards to improve the efficiency and effectiveness of the country's health care system. HIPAA applies such practices to all health care providers in the United States and strengthens penalties for violations.

Slide 7 – What are the specific HIPAA rules?

What are the specific HIPAA rules?


HIPAA Security Rule

- Sets national standards for the security of protected health information

HIPAA Privacy Rule

- Protects the privacy of individually identifiable health information

DOH Mandatory Training FY2013-2014



There are only two HIPAA rules, and they guide DOH information security and privacy. The first is the HIPAA Security Rule. It sets national standards for the security of protected health information. The second is the HIPAA Privacy Rule. It protects the privacy of individually identifiable health information.

Slide 8 – What are the specific HIPAA rules?


What are the specific HIPAA rules?

HIPAA Privacy Rule

- Sets boundaries on use & release of health records
- Holds people accountable if they violate patient rights
- Provides complaint mechanism for non-compliance
- Safeguards protected health information (PHI) for individually identifiable health information

All employees must comply with HIPAA rules

DOH Mandatory Training FY2013-2014



The HIPAA Privacy Rule sets boundaries on the use and release of health records. It is designed to hold people accountable if they violate patient rights. This rule provides complaint mechanisms for non-compliance and safeguards protected health information (PHI) that refers to individually identifiable health information.

All employees **must** comply with HIPAA. You can get more information from the U.S. Department of Health & Human Services.



Slide 9 – Federal and State Policies and Regulations

Federal & State Policies & Regulations

- **Public Law 111-5** - The American Recovery & Reinvestment Act of 2009
- **Title 45 Code of Federal Regulations** - Federal law governing the operations & existence of the Department
- **Chapter 119.07, F.S.** - Defines a public record, the public's right of access, retention requirements & exceptions to the rule
- **Chapter 282.318, F.S.** - Establishes Department's information security program & requirements



DOH Mandatory Training FY2013-2014

The Department's Information Security and Privacy Policy is governed by a number of federal and state rules, statutes and regulations. All employees should be familiar with this legislation.

We will list some of these rules and regulations, and then explain the more important ones specifically. The rules, statutes, and regulations include, but are not limited, to the following:

- **Public Law 111-5**, The American Recovery and Reinvestment Act of 2009
- **Title 45 Code of Federal Regulations** is the federal law governing the operations and existence of the Department of Health through the Department of Health and Human Services
- **Chapter 119.07, Florida Statute**, which defines a public record, the public's right of access, retention requirements and the exceptions to the rule and
- **Chapter 282.318, Florida Statute**, which establishes the Department's information security program and requirements

Slide 10 – Federal and State Policies and Regulations

Federal & State Policies & Regulations

- **F.A.C. 60DD** - Rules concerning the State Technology Office
- **Chapter 815, F.S.** – defines *Florida Computer Crimes Act* & the penalties for violation of this act. This chapter prohibits:
 - Introduction of fraudulent records into a computer system
 - Unauthorized use of computer facilities
 - Alteration or destruction of computerized information
 - Stealing of data from computer files



DOH Mandatory Training FY2013-2014

Florida Administrative Code 60DD is the rule established by the Department of Management Services concerning the State Technology Office; and finally,

Chapter 815, Florida Statute, which defines the *Florida Computer Crimes Act* and the penalties for violation of this act. It 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.

Members of the DOH workforce who have access to a work computer and confidential information should be familiar with these policies.




Slide 11 – Florida Public Records Act, Chapter 119.07, F.S.

Florida Public Records Act Chapter 119.07, F.S.

- All state, county & municipal records are open for personal inspection & copying by any person
- Each agency is responsible for providing access to public records

All DOH employees must comply with this Act



DOH Mandatory Training FY2013-2014

Let's look at each rule and regulation in order to comprehend the basics. We will start with the Florida Public Records Act, Chapter 119.07, Florida Statute.


Chapter 119.07, Florida Statute, states that all state, county and municipal records are open for personal inspection and copying by any person, and each agency is responsible for providing access to public records. All DOH employees must comply with the Florida Public Records Act.

Slide 12 – Florida Public Records Act

Florida Public Records Act

What records are & are not exempt from public disclosure? Refer to:

- Public Records Request Policy, DOHP 30-1
- DOH Employee Handbook
- Health Information Management Training Guidelines



DOH Mandatory Training FY2013-2014

The Public Records Act allows that some public records are exempt from disclosure. In order to determine which records are and are not exempt from public disclosure, you can use the following resources:

- The Public Records Request Policy, DOHP 30-1
- The DOH Employee Handbook and
- The Health Information Management Training Guidelines



Slide 13 – Enterprise Security of Data and Information Technology Act, Chapter 282.318, F.S.

Enterprise Security of Data & Information Technology Act,

Chapter 282.318, F.S.

The State Technology Office:

- Consults with each state agency head
- Is responsible & accountable for assuring adequate level of security for all agency data & information technology resources



DOH Mandatory Training FY2013-2014

The next statute we will cover is the Enterprise Security of Data and Information Technology Act, Chapter 282.318, Florida Statute. Information resources are valuable assets of the state and as such should be managed effectively. The Enterprise Security of Data and Information Technology Act states that the State Technology Office, in consultation with each state agency head, is responsible and accountable for assuring an adequate level of security for all data and information technology resources of each agency.

Slide 14 – Enterprise Security of Data and Information Technology Act

Enterprise Security of Data & Information Technology Act

Each agency is responsible for the following:

- Designate an information security manager
- Conduct & update a comprehensive risk analysis
- Develop & update written internal policies & procedures



DOH Mandatory Training FY2013-2014

Under the Enterprise Security of Data and Information Technology Act, each agency is responsible for the following:

- Designation of an information security manager, who shall administer the agency security program
- Conduct and update a comprehensive risk analysis to determine the security threats to the data and information technology resources and
- To develop and update written internal policies and procedures to assure the security of agency resources

Slide 15 – Enterprise Security of Data and Information Technology Act

Enterprise Security of Data & Information Technology Act

Additional Agency responsibilities:

- Implement appropriate cost-effective safeguards
- Ensure that periodic internal audits & evaluations of the security program
- Include appropriate security requirements in written specifications for procuring resources & services



DOH Mandatory Training FY2013-2014

Additional agency responsibilities under the Enterprise Security of Data and Information Technology Act are to:

- Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks
- Ensure that periodic internal audits and evaluations of the security program are conducted
- Include appropriate security requirements in written specifications for the solicitation and procuring of information technology resources and services

Slide 16 – Florida Computer Crimes Act, Chapter 815, Florida Statute

Florida Computer Crimes Act Chapter 815, F.S.

Prohibits the following:

- Introduction of fraudulent records into a computer system
- Unauthorized use of computer facilities
- Alteration or destruction of computerized information
- Stealing of data from computer files

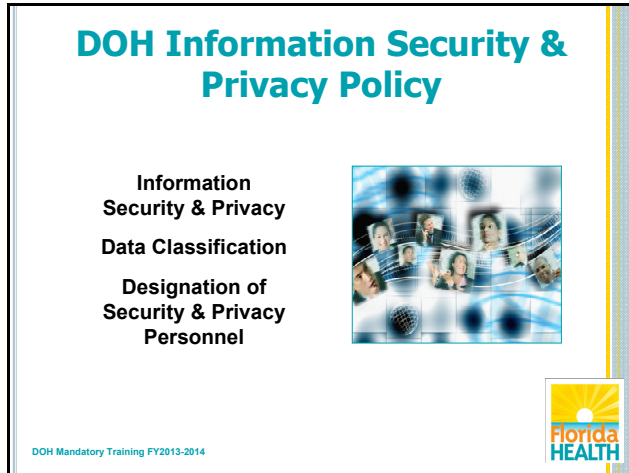


DOH Mandatory Training FY2013-2014

The Florida Computer Crimes Act, Chapter 815, Florida Statute, prohibits the following:



- Introduction of fraudulent records into a computer system
- Unauthorized use of computer facilities
- Alteration or destruction of computerized information
- Stealing of data from computer files

Slide 17 – DOH Information Security and Privacy Policy



DOH Information Security & Privacy Policy

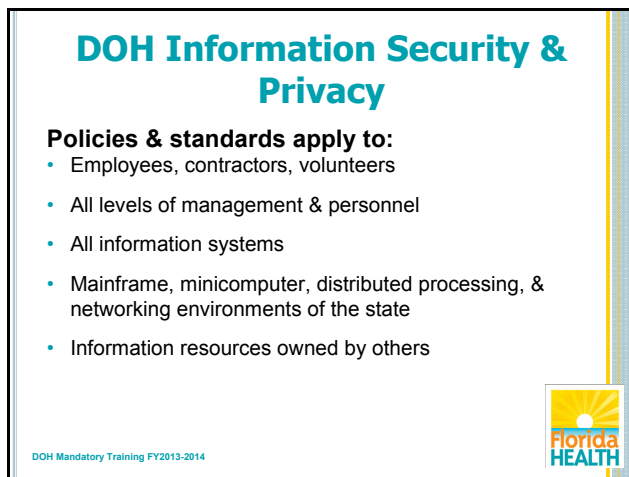
- Information Security & Privacy
- Data Classification
- Designation of Security & Privacy Personnel



DOH Mandatory Training FY2013-2014

Now that we have discussed the specific federal and state, regulations and statutes that support the Department's information security and privacy policy, let's become familiar with the three key sections of this policy: Information Security and Privacy; Data Classification; Designation of Security and Privacy Personnel.


Slide 18 – DOH Information Security and Privacy



DOH Information Security & Privacy

Policies & standards apply to:

- Employees, contractors, volunteers
- All levels of management & personnel
- All information systems
- Mainframe, minicomputer, distributed processing, & networking environments of the state
- Information resources owned by others



DOH Mandatory Training FY2013-2014

Information security policies and standards apply to:

- All members of the Department of Health workforce, including employees, contractors, and volunteers
- All levels of management and personnel
- All information systems that access, process, or have custody of data including automated information systems
- Mainframe, minicomputer, distributed processing and networking environments of the state, and
- They also 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 responsibility to protect the resources while in the custody of the state

Slide 19 – Information Security and Privacy Section

Information Security & Privacy Section

- Covers the protection of state information resources
- Information Resource Security Program or Information Technology Resource Program must:
 - Prevent, detect, contain, appropriately report, & correct security violations
 - Be responsive & adaptable to changing environments, vulnerabilities & technologies
 - Help create written local information security & privacy procedures to ensure security

DOH Mandatory Training FY2013-2014



This policy section covers the protection of state information resources from unauthorized modification, destruction, or disclosure, whether accidental or intentional.

The Information Resource Security Program or Information Technology Resource Program must:

- Prevent, detect, contain, appropriately report, and correct security violations
- Be responsive and adaptable to changing environments, vulnerabilities and technologies affecting state information resources
- Help create written local information security and privacy procedures to ensure the security of information and protect confidentiality, data integrity and access to information for each DOH division, program area, CHD and CMS area office

Slide 20 – Data Classification Section

Data Classification Section

- Public or confidential information in accordance with applicable state & federal laws & statutes
- 3 types of data:
 1. **Public:** All DOH data or information, **except** for those exempted from disclosure by state statute
 2. **Confidential:** All data or information which is exempt from disclosure by state statute, or designated as confidential by federal law, including protected health information
 3. **Exempt:** Statutory exceptions to Public Records Law & other portions of Florida laws

DOH Mandatory Training FY2013-2014



The Data Classification section covers data classification as public or confidential information in accordance with state and federal laws and statutes. Per DOH policy, data is separated into three types:

1. **Public information** – This includes all data or information from DOH divisions, offices, county health departments, and CMS area offices, except when specifically exempted from disclosure by state statute.
2. **Confidential information** – This is all data or information which is exempt from disclosure by state statute, or designated as confidential by federal law, including protected health information; and finally,
3. **Exempt information** – This includes Statutory exceptions to the Public Records Law and other portions of Florida laws and statutes.

Slide 21 – Designation of Security and Privacy Personnel Section

Designation of Security & Privacy Personnel Section

Each division, office, CHD & CMS is responsible for local information security & privacy

- Key personnel must be designated
- Identity of designees must be documented
- Eleven designations of security & privacy personnel



DOH Mandatory Training FY2013-2014

The Designation of Security and Privacy Personnel section covers the responsibility of each DOH division, office, county health department and CMS area office for the security and privacy of information within its jurisdiction. To accomplish this, key personnel with specific responsibility must be designated to coordinate the security and privacy of information. The identity of the designees must be documented in the local information security and privacy procedures, and their responsibilities must be included in the position description.

There are eleven designations of security and privacy personnel. These designations will be explained in the following two slides.

Slide 22 – Designation of Security and Privacy Personnel Section

Designation of Security & Privacy Personnel Section

11 designations of security & privacy personnel, 1-6

1. The State Surgeon General
2. The HIPAA Privacy Officer
3. The HIPAA Complaint Officer
4. The Information Security Manager
5. The HIPAA Security Officer
6. DOH Division Directors/Administrators



DOH Mandatory Training FY2013-2014

The first six designations of security and privacy personnel are as follows:


1. **The State Surgeon General** is ultimately responsible for the implementation of information security and privacy policies, protocols, and procedures. This includes designating headquarters' security officials such as the HIPAA Privacy Officer, the HIPAA Privacy Complaint Officer, the Information Security Manager, and the HIPAA Security Officer.
2. **The HIPAA Privacy Officer** provides leadership for the development of policies and procedures.
3. **The HIPAA Privacy Complaint Officer** functions as the HIPAA Privacy Complaint Officer for all privacy violations.
4. **The Information Security Manager** is responsible for administering the Department's Data and Information Technology Security Program.
5. **The HIPAA Security Officer** administers the Department's Data and Information Technology Security Program and the HIPAA Security Rule.
6. **DOH Division Directors and Administrators** designates the Local Information Security and Privacy Coordinators.

Slide 23 – Designation of Security and Privacy Personnel Section

Designation of Security & Privacy Personnel Section

11 designations of security & privacy personnel, 7-11

7. Information Resource Owners
8. Local Information Security & Privacy Coordinators
9. Local HIPAA Reviewing Officer
10. Local Information Custodian
11. Local IT Disaster Recovery Coordinator



DOH Mandatory Training FY2013-2014


The next five of the eleven designations are:

7. **Information Resource Owners** specify the security properties.
8. **Local Information Security and Privacy Coordinators** are central points of contact for other staff that are assigned information security and privacy duties.
9. **Local HIPAA Reviewing Officer**, often a physician who reviews any individual's complaint on a decision.
10. **Local Information Custodian** establishes procedures in accordance with Department of Health policies, protocol, and procedures.
11. **Local IT Disaster Recovery Coordinator** plans and directs detailed information technology activities before, during, and after a disaster.

Slide 24 – End Slide

End of Information Security & Privacy Awareness Training Section 1

Return to the course
& begin Section 2



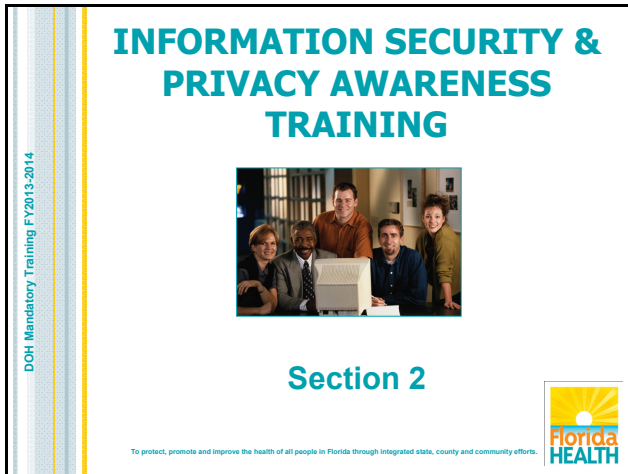
To protect, promote and improve the health of all people in Florida through integrated state, county, and community efforts.

This concludes Section 1 of Information Security and Privacy Awareness Training. Please return to the course and begin Section 2.



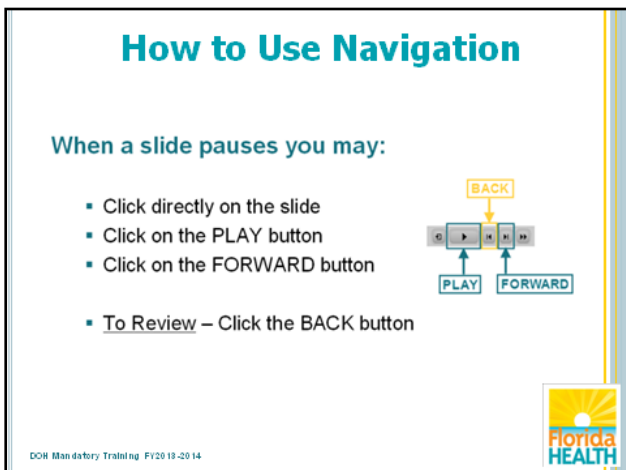
Section 2

Slide 1 – Welcome Slide



Hello, and welcome to Section 2 of Information Security and Privacy Awareness Training. In this section, we will explain more key sections of the DOH Information Security and Privacy policy.

Slide 2 – How to Use Navigation



In order to make your training experience as easy as possible during the course of this self-paced DOH Mandatory Training course, we are providing these navigation instructions.

When a slide pauses you can do one of three things to advance the presentation:

- You may click directly on the slide with your cursor
- You may click on the PLAY button on the bottom left of the screen
- or
- You may click on the FORWARD button, also located on the bottom left of the screen

If you need to review a previous slide you may click the BACK button on the bottom left of the screen. Please keep these instructions in mind as you proceed with this training. You will need to advance the slide now.




Slide 3 – Section 2 Objectives

Section 2 Objectives

Identify DOH Information Security & Privacy Policy Sections:

1. Acceptable Use & Confidentiality Agreement
2. Security & Privacy Awareness Training
3. Secured Areas & Physical Security Procedures
4. Confidential Information
5. Disclosure of Confidential Information



DOH Mandatory Training FY2013-2014

Upon completion this section, you will be able to identify the following sections of the Department of Health's Information Security and Privacy policy:

1. Acceptable Use and Confidentiality Agreement
2. Security and Privacy Awareness Training
3. Secured Areas and Physical Security Procedures
4. Confidential Information and
5. Disclosure of Confidential Information

Slide 4 – DOH Information Security and Privacy Policy

DOH Information Security & Privacy Policy



- Acceptable Use & Confidentiality Agreement
- Security & Privacy Awareness Training
- Secured Areas & Physical Security Procedures



DOH Mandatory Training FY2013-2014

The following slides will review the sections regarding the acceptable use and confidentiality agreement; security and privacy awareness training; and procedures for secured areas and physical security.



Slide 5 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

- Covers protecting information from unauthorized modification, destruction, use or disclosure & safeguarding confidential information
- All members of the workforce are responsible for protecting information
- All DOH data, information & technology resources to be used only for state business
- Supervisors may monitor computer use – observation, reviewing history & productivity

DOH Mandatory Training FY2013-2014



The Acceptable Use and Confidentiality Agreement section covers protecting information from unauthorized modification, destruction, use or disclosure and safeguarding confidential information. All members of the workforce shall be held accountable for protecting information as stated in this policy. All DOH data, information and technology resources shall only be used for official state business. Supervisors may monitor computer use by direct observation, reviewing computer history files through the systems administrator, or reviewing work productivity and quality.

Slide 6 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

- Only authorized IT personnel can install DOH approved software & hardware
- No expectation of privacy while using DOH resources
- Written approval is required to use streaming media technologies

DOH Mandatory Training FY2013-2014



Per this policy section, only authorized IT personnel can install DOH-approved software and hardware. Employees should have no expectation of privacy while using Department resources. To use streaming media technologies, you must receive written approval from your supervisor and the Information Security Manager or delegate.



Slide 7 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Access to the internet, telephone systems, or email service at DOH is a privilege, not a right

- Adhere to Department policies & procedures, as well as local, state & federal laws & regulations
- Supervisors will regularly review the access privileges of staff to ensure access is appropriate to job responsibilities



DOH Mandatory Training FY2013-2014

Keep in mind that access to the Internet, telephone systems, or email service is a privilege, not a right. As a Department employee, you must adhere to Department policies and procedures, local and state laws, as well as federal laws and regulations. It is important to note that supervisors will regularly review the access privileges of staff to ensure access is appropriate to job responsibilities.

Slide 8 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Computer Use

- DOH employees will have a user account
- Log off or lock your workstation/computer when leaving
- Secure workstations/computers with a password protected screensaver
- Respect & obey copyright laws regarding use or duplication of software



DOH Mandatory Training FY2013-2014

The technology rules and regulations regarding computer use by DOH employees and staff are also covered in this section of the policy and are very important to the everyday functions of the Department. DOH employees are given a user account to access DOH information technology resources. Be sure to log off or lock your workstation or computer prior to leaving the work area. Your workstation or computer must be secured with a password-protected screensaver. Set the automatic activation feature for a delay of no more than 10 minutes. The Department and its employees shall respect the legitimate proprietary interests of intellectual property holders and obey the copyright law prohibiting the unauthorized use or duplication of software



Slide 9 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Computer Use

- Personal passwords may not be shared or disclosed, do not include passwords in e-mails
- Staff held accountable for all activities under their DOH user ID or password
- Change network passwords every 30 days
- Passwords should be at least 8 characters long, including letters & numbers



DOH Mandatory Training FY2013-2014

The password for your computer is an important aspect of information security. Your user account grants access to DOH information technology resources. This access is based on the documented need provided by the appropriate hiring authority.

Anyone who has or is responsible for a user account within the Department's network must take the appropriate steps to select and secure their passwords. It is your responsibility to take appropriate steps to select and secure your password. Password protection is important. Following these simple guidelines will help keep your computer and its data secure:

- Personal passwords may not be shared or disclosed. Do not include passwords in e-mails.
- Staff will be held accountable for all activities that occur under their DOH user ID or password.
- Network passwords must be changed every 30 days.
- For better security passwords should be at least 8 characters long, including letters and numbers.

Slide 10 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Computer Use – Permitted Activities

- Visiting non-DOH-prohibited internet sites
- Email for personal reasons during non-work hours
- Access to non-DOH-browser email accounts



DOH Mandatory Training FY2013-2014

As a Department employee, your computer is to be used primarily to accomplish your job duties and responsibilities. The Information Security and Privacy policy does allow for access to non-work related sites, but you must follow the guidelines for permitted and prohibited computer activities.

Permitted activities include:

- Visiting non-DOH-prohibited internet sites
- The use of email for personal reasons during non-work hours within the limitations contained in this policy and
- Access to non-DOH-browser based email accounts, such as AOL or Yahoo

However, these permitted activities must not interfere with your job duties, must not be used excessively and must not compromise the DOH network.



Slide 11 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Computer Use – Prohibited Activities

- Install unlicensed or unapproved software
- Introduce viruses, worms, trojan horses, email bombs, etc.
- Access or download inappropriate material
- Access non-work related chat rooms
- Program emails to forward to a non-DOH email address

DOH Mandatory Training FY2013-2014



Per the Information Security and Privacy policy, prohibited activities include, but are not limited to:

- Installing, introducing, downloading, accessing, or distributing any unlicensed software or software not approved by the DOH Information Technology Standard Workgroup
- Introducing viruses, worms, trojan horses, email bombs, etc. through willful intent or negligence
- Accessing or downloading inappropriate material
- Accessing non-work related chat rooms, news groups, political groups, singles clubs, or dating services
- Programming email to automatically forward messages to an external destination outside the Department's network

Slide 12 – Acceptable Use and Confidentiality Agreement Section

Acceptable Use & Confidentiality Agreement Section

Computer Use – Prohibited Activities

- Do not access unauthorized confidential/proprietary information
- Do not connect a DOH laptop to a non-DOH wireless network
- Do not erase, destroy or hide web browsing audit trails
- Do not disable, alter or circumvent Department workstation security measures

DOH Mandatory Training FY2013-2014



Do not access unauthorized confidential/proprietary information.

Do not connect a DOH laptop to a non-DOH wireless network.

Do not erase, destroy or hide web browsing audit trails.

Do not disable, alter or circumvent Department workstation security measures.

If a DOH employee must perform any of these prohibited activities as part of their job duties and responsibilities, they must have written supervisory



Slide 13 – Security and Privacy Awareness Training Section

Security & Privacy Awareness Training Section

DOH employees must receive security & privacy awareness training prior to accessing the DOH network.

Before you:

- Provide services to clients
- Access confidential information
- Access information technology

This training meets these requirements!



DOH Mandatory Training FY2013-2014

The Security and Privacy Awareness Training section of this policy requires that DOH employees must receive initial security and privacy awareness training prior to accessing the DOH network. This includes access used for providing services to clients, accessing confidential information and accessing information technology.


Additionally, employees are required to take the annual update to the information security and privacy awareness training course. The training you are now taking meets these requirements.

Slide 14 – Secured Areas and Physical Security Procedures Section

Secured Areas & Physical Security Procedures Section

Secured Areas

- Designate & maintain secured areas for the security & privacy of information
- Protect confidentiality & data integrity
- Provide appropriate access to information using administrative, physical & technical controls
- Document each designated secured area in the local information security & privacy procedures
- Access only provided to those members with documented “need-to-know” authorization



DOH Mandatory Training FY2013-2014

As stated in the Secured Areas and Physical Security Procedures policy section, the Department must designate and maintain secured areas to ensure the security and privacy of information and information technology resources. This is to protect confidentiality and data integrity. The Department must also 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.

Access to the secured areas should only be provided to those members with documented “need-to-know” authorization. For example, an employee who is responsible for billing Medicaid for a child’s health assessment does not need to have the child’s full medical record or even the assessment results. He or she only needs to know the information required to process the payment and will be provided the minimum necessary information to do the job.




Slide 15 – Secured Areas and Physical Security Procedures Section

Secured Areas & Physical Security Procedures Section

Physical Security Procedures

- Visitors must always be escorted in secured areas
- Secured areas must have a reliable locking system
- Reliable locking systems must be used. Electronic locks must have a manual locking system as back-up
- Access should be limited to a documented list of authorized staff



DOH Mandatory Training FY2013-2014

Physical security of secured areas is very important to prevent possible security breaches. Here are the procedures for the physical security of DOH secured areas:

- Visitors must always be escorted by an authorized DOH employee in secured areas.
- Secured areas must have reliable locking systems and construction that does not allow unauthorized access. If an electronic locking system is used, a reliable manual locking system must be in place as a back-up, in the event of a power outage.
- Access to the secured area should be limited to a documented list of authorized staff, and procedures for removing and returning the information must be in place.

Slide 16 – Secured Areas and Physical Security Procedures Section

Secured Areas & Physical Security Procedures Section

Physical Security Procedures

- For each secured area, a key custodian & alternate key custodian must be designated
- Access logs must be kept for staff needing temporary access to secured areas
- Any modifications or repairs to secured areas are to be coordinated with the local information custodian

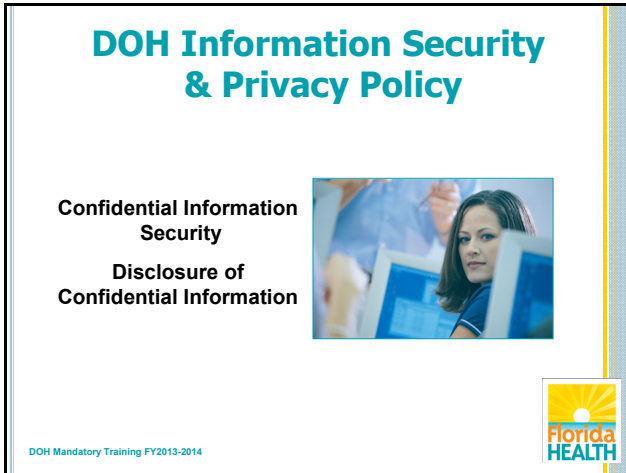


DOH Mandatory Training FY2013-2014

For each secured area, a key custodian and alternate key custodian must be designated. They are responsible for maintaining control of the keys, providing access to authorized staff and annually updating the inventory of information resources and information sets maintained in the designated secured area. Access logs must be kept and maintained for those persons that need temporary or occasional access but are not issued a key for each secured area. Any modifications or repairs to secured areas are to be coordinated with the local information custodian to document the actions being taken.





Slide 17 – DOH Information Security and Privacy Policy



DOH Information Security & Privacy Policy

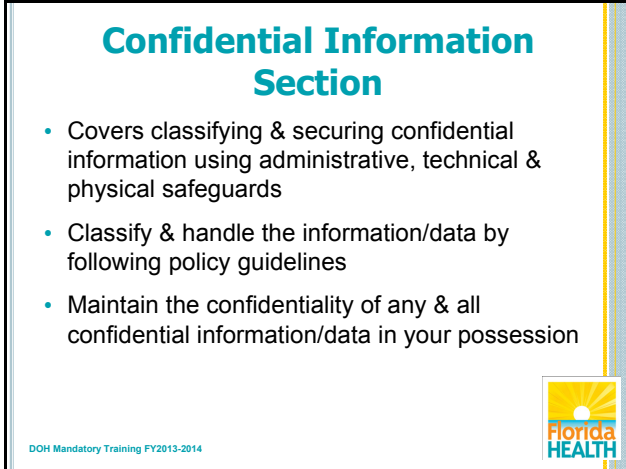
Confidential Information Security
Disclosure of Confidential Information



DOH Mandatory Training FY2013-2014


Recall from Section 1 of this course that information is classified as either public or confidential. The next section of this presentation will review the sections of the Information Security and Privacy policy regarding confidential information security and disclosure of confidential information. It is very important to make note of the regulations pertaining to confidential information, as violations of these regulations may result in disciplinary action.

Slide 18 – Confidential Information Section



Confidential Information Section

- Covers classifying & securing confidential information using administrative, technical & physical safeguards
- Classify & handle the information/data by following policy guidelines
- Maintain the confidentiality of any & all confidential information/data in your possession



DOH Mandatory Training FY2013-2014

The Confidential Information Section covers the classifying and securing of confidential information by using appropriate administrative, technical and physical safeguards. All DOH employees should be able to classify and handle data or information using these guidelines. You are responsible for maintaining the confidentiality of any and all confidential information or data in your possession. The next slide details some of the policy guidelines for protecting confidential information.




Slide 19 – Confidential Information Section

Confidential Information Section

To protect confidential information:

- Position computer monitors to prevent viewing
- Designated people for file transfer from database
- Consultations involving confidential information in areas with restricted access
- Electronic transmission of confidential information must be encrypted
- Data back-ups must be locked in a secured area
- Do not use laptops to store any type of information



DOH Mandatory Training FY2013-2014

To protect confidential information, position computer monitors to prevent unauthorized viewing. A person or persons shall be designated in the local operating procedures as responsible for the electronic file transfers of information from confidential databases. Consultations involving confidential information, such as information regarding employees and/or clients, or any other confidential information, must be held in areas with restricted access

Please note - Discussions about employees and/or clients must be limited to information necessary to provide care or perform job functions. It is also important to note that access to reports and files, which contain patient identifying information for reasons other than treatment, payment and operations must be logged, tracked and periodically audited.


Electronic transmission of confidential information must be encrypted. Data back-ups must be locked in a secured area. Do not use laptop computers to store any typed of information, confidential or otherwise.

Slide 20 – Confidential Information Section

Confidential Information Section

Telephone Communication Procedures

- Conduct conversations in private areas where they cannot be overheard
- Cell phones are not secure – advise the caller of cell phone use
- Determine caller identity before releasing any information



DOH Mandatory Training FY2013-2014

The Confidential Information Section also covers procedures for handling confidential information via telephone, mail, fax and e-mail. This slide and the following four slides will address these procedures.

Telephone communication procedures include conducting discussions of confidential information by phone in private areas where the conversation cannot be overheard. Cell phones are not considered to be secure. Employee-initiated cell phone calls regarding confidential information should be limited to the minimum amount of information necessary. The person called should be advised that the discussion is taking place on a cell phone and the conversation is not guaranteed to be secure. The employee must determine the identity of the caller and what information can be disclosed to that person before releasing any information.




Slide 21 – Confidential Information Section

Confidential Information Section

Mailing Confidential Information

- Secure mail intake sites for all incoming confidential mailings
- Secure mailrooms & mailboxes
- Double enveloping is required:
 - The outside envelope addressed to recipient
 - The inside envelope is marked confidential & specifies the recipient



DOH Mandatory Training FY2013-2014

Mailing confidential information procedures include the following:


- A secured mail intake site must be used to receive incoming confidential information, such as laboratory results, patient medical records, or surveillance case reports.
- Mailrooms and mailboxes must be secured to prevent unauthorized access to incoming or outgoing mail.
- Double enveloping is required when mailing confidential or sensitive information. The outside envelope is addressed to the recipient, and the inside envelope is marked confidential and specifies the recipient.

Slide 22 – Confidential Information Section

Confidential Information Section

Faxing Confidential Information

- Keep fax machines in secured area with limited visual access
- Before faxing, obtain consent & authorization to release the confidential information
- Use a cover sheet marking the fax as confidential – must include specific text



DOH Mandatory Training FY2013-2014

Confidential information may be faxed using appropriate administrative, technical and physical safeguards. Faxing confidential information procedures include keeping fax machines designated to receive and transmit confidential information in a secured area with limited visual and physical access. Before faxing any confidential information such as employee, client, or medical information, you must obtain proper consent, authorization and release permissions. The designated information custodian for confidential information is responsible for the release of information from the specific information set. When faxing, you must use a cover sheet that specifically marks the fax transmission as “Confidential”. Specific text must also be on the cover sheet; this text is provided in the next slide.



Slide 23 – Confidential Information Section

Confidential Information Section

Confidential Fax Cover Sheet Text

This transmission may contain material that is CONFIDENTIAL under federal law & Florida Statutes & 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 & 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.

DOH Mandatory Training FY2013-2014



A fax cover sheet marked “Confidential” and containing the following paragraph must accompany all 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.

Slide 24 – Confidential Information Section

Confidential Information Section

E-mail Procedures

- E-mail is generally public record & archived by the Department
- E-mail must be reviewed & confirmed by the General Counsel's Office prior to release
- E-mails containing confidential information must be encrypted, including any attachments

DOH Mandatory Training FY2013-2014



E-mail is generally considered public record, and archived copies are kept by the Department. However, all e-mail must be reviewed and confirmed as a public record by the General Counsel's Office prior to release. Confidential information cannot be sent by e-mail unless encryption is used for the e-mail and any attachments.



Slide 25 – Disclosure of Confidential Information Section

Disclosure of Confidential Information Section

- Covers disclosure of confidential information exempt from public disclosure & how to ensure its protection
- All records maintained by the Department are public records
- Available for inspection or copying by the public under the supervision of Department personnel with certain exceptions
- Charges may not exceed that specified in the public records law

DOH Mandatory Training FY2013-2014



The Disclosure of Confidential Information section covers disclosure of confidential information which is exempt from public disclosure by state or federal law, rule, or regulation, and how to ensure its protection in accordance with these protocols. All records maintained by the Department of Health are public records. They are available for inspection or copying by the public at reasonable times under the supervision of Department personnel with certain exceptions. A charge for copying, preparing or searching a record for inspection may not exceed that specified in the public records law.

Slide 26 – Disclosure of Confidential Information Section

Disclosure of Confidential Information Section

Exceptions to public access of public records:

- Client Eligibility Applications:
 - Bank account numbers
 - Debit card numbers
 - Credit card numbers
- Sealed Bids or Proposal
- Financial Statements
- Computer Software

DOH Mandatory Training FY2013-2014



There are exceptions to public access to public records due to the confidential nature or security issues that appear in numerous places throughout the state and federal statutes. These exceptions are designated as confidential or non-disclosable. Some of these exceptions are:

- **Client Eligibility Applications**, which include all personal identifying information, bank account numbers, debit and credit card information contained in records relating to an individual's personal health or eligibility for health-related services
- **Sealed bids or proposals** that are received by the Department, which are not disclosable until the award date or 10 days after the opening
- **Financial statements** received by the Department for bid pre-qualifying and
- **Computer software**, which includes commercially available programs and data processing under a licensing agreement

Slide 27 – Disclosure of Confidential Information Section

Disclosure of Confidential Information Section

**Exceptions to public access of personnel files:
Confidential or non-disclosable information,
such as**

- Social Security Numbers
- Location information
- Complaints of discrimination
- Medical information



DOH Mandatory Training FY2013-2014

Exceptions to public access regarding information contained in personnel files of state employees are generally accessible by the public. There are certain exceptions that are designated as confidential or non-disclosable. Some of these are:

- **Social Security Numbers**, which 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
- **Location information**, including but not limited to, home addresses, telephone numbers, social security numbers, photographs and daycare information for the following people or their spouse: department personnel supporting abuse investigations, human resource employees, labor relations employees, assistant directors, managers, or assistant managers of any government agency
- **Complaints of discrimination** relating to race, color, religion, national origin, age, handicap, or marital status are confidential and not disclosable; and finally,
- **Medical information** pertaining to a prospective, current, or former officer or employee of an agency



Slide 28 – End Slide

End of Information Security & Privacy Awareness Training Section 2

Return to course & begin Section 3

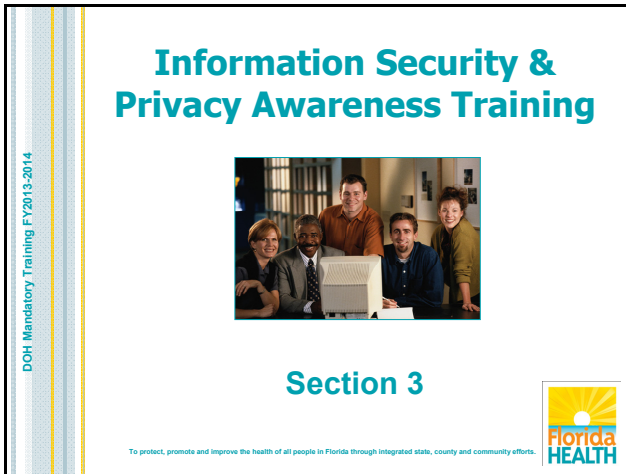
To protect, promote and improve the health of all people in Florida through integrated state, county, and community efforts.

This concludes Section 2 of Information Security and Privacy Awareness Training. Please return to the course and begin Section 3.



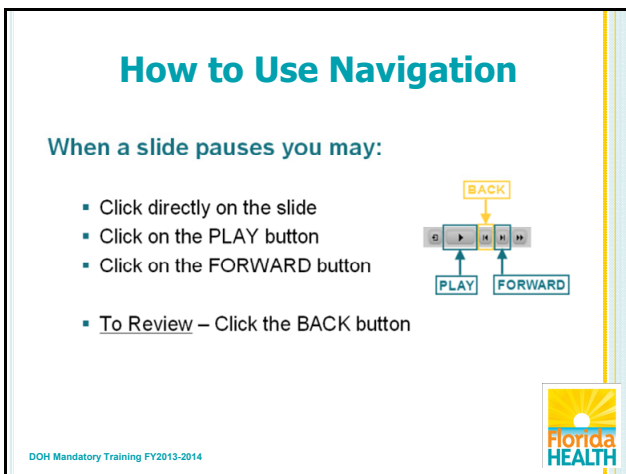
Section 3

Slide 1 – Welcome Slide



Hello, and welcome to Section 3 of the Department of Health's Information Security and Privacy Awareness Training. In this section, we will continue explaining the key sections of the DOH Information Security and Privacy policy.

Slide 2 – How to Use Navigation



In order to make your training experience as easy as possible during the course of this self-paced DOH Mandatory Training, we are providing these navigation instructions.

- When a slide pauses you can do one of three things to advance the presentation:
- You may click directly on the slide with your cursor
- You may click on the PLAY button on the bottom left of the screen
or
- You may click on the FORWARD button, also located on the bottom left of the screen

If you need to review a previous slide you may click the BACK button on the bottom left of the screen.

Please keep these instructions in mind as you proceed with this training. You will need to advance the slide now.




Slide 3 – Section 3 Objectives

Section 3 Objectives

Identify the following DOH Information Security & Privacy Policy Sections:

1. Patient Privacy Rights
2. Public Health HIPAA Exemptions
3. Contract Providers & Business Associates
4. Retention, Achieving & Disposition of Records
5. Risk Analysis
6. Contingency Planning
7. Information Resource Management Security



DOH Mandatory Training FY2013-2014

Upon completion this section, you will be able to identify the following sections of the Department of Health's Information Security and Privacy Policy:

1. Patient Privacy Rights
2. Public Health HIPAA Exemptions
3. Contract Providers and Business Associates
4. Retention, Achieving and Disposition of Records
5. Risk Analysis
6. Contingency Planning and
7. Information Resource Management Security

Slide 4 – DOH Information Security and Privacy Policy

DOH Information Security & Privacy Policy



1. Patient Privacy Rights
2. Public Health HIPAA Exemptions
3. Contract Providers & Business Associates



DOH Mandatory Training FY2013-2014

The following slides will review the sections regarding patient privacy rights, public health HIPAA exemptions, and contract providers and business associates.



Slide 5 – Patient Privacy Rights Section

Patient Privacy Rights Section

- Standards established to protect the privacy of medical records & protected health information
- HIPAA supports the DOH-established privacy standards
- HIPAA improves the efficiency & effectiveness of the country's health care system
- HIPAA helps health care providers eliminate waste, streamline & expand potential

DOH Mandatory Training FY2013-2014



The Patient Privacy Rights Section covers information security policies and procedures relating to patients' rights. To prevent the misuse of individually identifiable health care information, standards must be established to protect the privacy and security of medical records and other protected health information.

HIPAA supports the DOH-established privacy standards. HIPAA is part of a plan to make the country's health care system more efficient and effective. HIPAA helps health care providers eliminate waste, streamline electronic transmission and expand the potential to share health information.

Slide 6 – Patient Privacy Rights Section

Patient Privacy Rights Section

HIPAA Privacy Rule

- Safeguards to protect privacy of health care information
- Sets boundaries on use & release of health records
- Holds people accountable if they violate patient rights
- Provides complaint mechanisms for non-compliance

DOH Mandatory Training FY2013-2014



The HIPAA Privacy Rule establishes the safeguards to ensure the confidentiality of protected health information. This means that any information that can be reasonably used to identify the health records of specific individuals must be protected. It sets boundaries on the use and release of health records, holds people accountable if they violate patient rights and provides complaint mechanisms for non-compliance. Everyone who works for the Department is responsible for following and enforcing the Department's security policy and HIPAA rules.



Slide 7 – Patient Privacy Rights Section

Patient Privacy Rights Section

Some Florida laws are more stringent than HIPAA requirements:

family planning

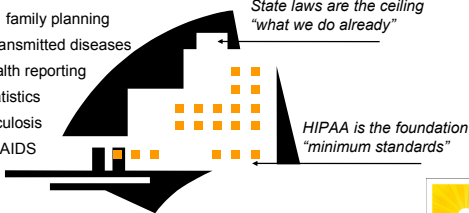
sexually transmitted diseases

public health reporting


vital statistics

tuberculosis

HIV/AIDS



DOH Mandatory Training FY2013-2014




The HIPAA Privacy Rule does not take away existing confidentiality rules as long as they are compatible with HIPAA, such as rules governing mandatory reporting of certain diseases and reporting for public health purposes. HIPAA establishes the minimum standards that must be met. It does not prevent a state from applying more restrictive policies and procedures to protect client privacy. In many instances, Florida laws are more stringent than HIPAA requirements.

Slide 8 – Patient Privacy Rights Section

Patient Privacy Rights Section

- Directs employees & volunteers to prevent unauthorized disclosure of protected health information
- Requires use of DOH forms that include HIPAA privacy language
- Provides DOH *Notice of Privacy Practices*
- Provides poster about client rights

DOH Mandatory Training FY2013-2014




The Patient Privacy Rights section of the DOH policy directs employees and volunteers to prevent unauthorized disclosure of protected health information, except as permitted or required by law. To assure client's rights, the policy requires the use of certain Department forms that have been revised to include HIPAA privacy language. Also provided by policy is a *Notice of Privacy Practices* and a poster about client rights.

Slide 9 – Patient Privacy Rights Section

Patient Privacy Rights Section

The DOH Notice of Privacy Practices

- Designed to inform clients about privacy rights
- The Department's duties to protect health information
- Explains when the Department may need permission to use client information
- Describes client's rights as they relate to the privacy of their health information
- How a client can file a grievance or complaint



DOH Mandatory Training FY2013-2014


The Florida Department of Health's *Notice of Privacy Practices* is a document designed to inform clients about their privacy rights. This notice includes the Department's duties to protect health information. It explains to the client why we may need to use or share their personal health information, when we need their permission to use or share it, and when we do not. The notice also describes the client's rights as they relate to the privacy of their health information and provides information about how to file a grievance or complaint if they feel their protected health information is being used improperly.

Slide 10 – Patient Privacy Rights Section

Patient Privacy Rights Section

The DOH Notice of Privacy Practices – Department of Health responsibilities

- Notifying all clients of their privacy rights
- Adopting & implementing privacy procedures
- Training staff on privacy procedures
- Ensuring business associates protect patient information
- Adopting privacy complaint procedures



DOH Mandatory Training FY2013-2014

It is the Department's duty to inform clients about the *Notice of Privacy Practices*. The Department is responsible for:

- Notifying all clients of the Department about their privacy rights under HIPAA
- Adopting and implementing privacy procedures
- Training staff on privacy procedures
- Ensuring business associates protect patient information under HIPAA and
- Adopting a privacy complaint process



Slide 11 – Patient Privacy Rights Section

Patient Privacy Rights Section

Rules regarding patient privacy

- Clients have the right to ask the Department to limit how it uses or discloses their protected health information
- The Department does not have to agree
- If a client's limits are denied, the client's record must be documented with reason for denial



DOH Mandatory Training FY2013-2014

Patient privacy rights include the following rules: the right to ask the Department to limit how it uses or discloses patient protected health information – except for those uses or disclosures that are required by law. However, even though the client can request that limits on use and disclosures be made, the Department does not have to agree to the client's restriction. In cases where a client's requested limits are denied, the client's records must be documented as to why the request was refused.

Slide 12 – Public Health HIPAA Exemptions Section

Public Health HIPAA Exemptions Section

- Addresses health information kept as a result of activities not covered by HIPAA Privacy Rule
 - **Exemption Example:** individual medical information recorded as a result of public health disaster, emergency, communicable disease surveillance or epidemiologic investigation
- Exemptions when *Notice of Privacy Practices* is not required & information is qualified as disclosable



DOH Mandatory Training FY2013-2014

The Public Health HIPAA Exemptions section addresses certain health information kept by the Department as a result of public health activities that are not covered by the HIPAA Privacy Rule. Individual medical information recorded as a result of a public health disaster, emergency, communicable disease surveillance or epidemiologic investigation are exempt from HIPAA.

There are also exemptions from the HIPAA Privacy Rule when the *Notice of Privacy Practices* is not required and certain public health information is qualified as disclosable.




Slide 13 – Public Health HIPAA Exemptions Section

Public Health HIPAA Exemptions Section

Example Activities with exempted information:

- Syndromic surveillance & surveillance of communicable diseases
- Epidemiologic investigations of communicable disease outbreaks & contact investigations
- Locating contacts for communicable disease prevention & regulatory activities



DOH Mandatory Training FY2013-2014

Some examples of activities that produce exempted information include:


- Syndromic surveillance and surveillance of communicable diseases or disease outbreaks
- Epidemiology investigations of communicable disease outbreaks and contact investigations
- Locating contacts for communicable disease prevention and regulatory activities

Slide 14 – Public Health HIPAA Exemptions Section

Public Health HIPAA Exemptions Section

Patient authorization is not required to disclose to the following registries:

- Tuberculosis
- Sexually Transmitted Diseases
- Cancer & Tumor
- Immunization
- Vital Statistics



DOH Mandatory Training FY2013-2014

Client or patient authorization for release of medical records is not required for the information to be disclosed to the following registries:

- Tuberculosis
- Sexually Transmitted Diseases
- Cancer and Tumor
- Immunization and
- Vital Statistics




Slide 15 – Public Health HIPAA Exemptions Section

Public Health HIPAA Exemptions Section

The law requires disclosure of medical records in response to:

- Child Abuse
- Neglect
- Domestic Violence
- Court orders
- Law enforcement officers
- Descendants
- Medical examiners
- Funeral directors



DOH Mandatory Training FY2013-2014


The law requires disclosure of medical records in cases such as suspected child abuse, neglect, or domestic violence, and in response to a court order or to a law enforcement officer, descendants, medical examiners, or funeral directors. If you are in doubt about sharing protected health information, check with your supervisor or the local DOH privacy officer.

Slide 16 – Contract Providers and Business Associates Section

Contract Providers & Business Associates Section

- Covers contract confidentiality & security of data, files & records related to contracts
- Contracts requiring access to confidential information must have standard contract language to implement security policy & procedures
- Contract providers with access to PHI must have a Business Associate Agreement
- The ITSW must be informed about contracts involving information technology

Questions? Contact your local contract manager



DOH Mandatory Training FY2013-2014

The Contract Providers and Business Associates section covers contract confidentiality and the security of all data, files and records, including client records, related to the contract. Each contract with the Department requiring the provider to have access to or produce confidential Department information must include standard contract language that requires the provider to implement policy and procedures to maintain confidentiality and security of all Department data, files and records related to the services detailed in the contract. Each contract provider that will have access to protected health information, or PHI, must have a Business Associate Agreement with the Department. All Department contracts involving information technology should be brought to the attention of the Information Technology Standards Workgroup, or ITSW.



If you have questions regarding contracts, contract providers, or Business Associate Agreements, please contact your local contract manager.



Slide 17 – DOH Information Security and Privacy Policy

DOH Information Security & Privacy Policy

- Retention, Archiving & Disposition of Records
- Risk Analysis
- Contingency Planning
- Information Resource Management Security



DOH Mandatory Training FY2013-2014


The following slides will review the final four sections of the Information Security and Privacy policy: Retention, Archiving, and Disposition of Records; Risk Analysis; Contingency Planning; and Information Resource Management Security

Slide 18 – Retention, Archiving and Disposition of Records Section

Retention, Archiving & Disposition of Records Section

- Covers Retention, archiving & destroying information in accordance with General Schedule for State Government
- General Schedule for State Government provides:
 - Guidelines for retention, transfer & disposition of public & confidential records
 - Standards established with legal, fiscal, historical & administrative value considered

Become familiar with the standards for confidentiality & security of records that you handle



DOH Mandatory Training FY2013-2014

The Retention, Archiving, and Disposition of Records policy section covers the retention, archiving and destroying of Department information in accordance with the General Schedule for State Government. The standards set by the General Schedule for State Government provides the Department with guidelines for the retention, transfer and disposition of public and confidential records taking into consideration their legal, fiscal, historical and administrative values. As a member of the DOH workforce, you must become familiar with the standards for the confidentiality, security of archiving and documenting procedures for the records you handle.




Slide 19 – Retention, Archiving and Disposition of Records Section

Retention, Archiving & Disposition of Records Section

For more information regarding Department standards:

- Contact your Local Records Management Liaison Officer
- Contact the Department's Records Manager
- Contact the Office of Information Technology
- Visit DOH Records Management Program website




DOH Mandatory Training FY2013-2014

For more information regarding the Department's Retention, Archiving, and Disposition of Records standards, contact your Local Records Management Liaison Officer, who is responsible for quality control of Department records for your division, program area, CHD or CMS. You may also contact the Department's Records Manager, contact the Office of Information Technology, or visit the DOH Records Management Program website.

Slide 20 – Risk Analysis Section

Risk Analysis Section

- Covers managing risks to data & information technology resources
- Risk to resources is determined through risk analysis
- Risk analysis should be performed annually
 - Must include a corrective action plan
 - Must use the DOH Information Security & Privacy Risk Assessment form
 - Cooperate on any corrective action needed



DOH Mandatory Training FY2013-2014


The Risk Analysis Section covers managing the risks to data and information technology resources. Risk to data and information technology resources is determined and handled through a risk analysis. A risk analysis should be performed annually and must include a corrective action plan. Documentation of the risk assessment and corrective action plan is confidential and not subject to public disclosure. To perform a risk analysis, designated DOH staff must use the current DOH Information Security and Privacy Risk Assessment form. It is your responsibility to cooperate with your local information custodian and local information security and privacy coordinator on any corrective actions resulting from the risk analysis.



Slide 21 – Contingency Planning Section

Contingency Planning Section

- Contingency plan provides essential functions & recovers critical information in the event of any disaster
- Contingency planning process:
 - Should identify critical functions
 - Should document practices for back up, storage & retrieval of electronically stored information
 - Should annually test the plans
 - Documentation shall be incorporated into local COOP & COOP-IT



DOH Mandatory Training FY2013-2014

The Contingency Planning section covers developing and adopting a written, cost-effective contingency plan to provide essential functions and recover critical information in the event of any disaster, natural or intentional.

The contingency planning process:

- Should identify critical functions
- Should document practices for the back up, storage and retrieval of electronically stored information
- Should annually test the plans and
- Documentation shall be incorporated into the local Continuity of Operations Plans, or COOP, and Continuity Operations for Information Technology Plans (COOP-IT), which are required by state and federal law

Slide 22 – Contingency Planning Section: Continuity of Operations for Information Technology Plans – COOP-IT Plan

Contingency Planning Section:

Continuity of Operations for Information Technology Plans – COOP-IT Plan


Local IT Disaster Recovery Coordinator

- Responsible for planning & directing detailed information technology activities
- Ensures implementation of local COOP-IT Plans

If you are involved in COOP:

- Be familiar with your responsibilities
- Be sure confidentiality of records is maintained
- Review & test plan annually

Questions? Contact your supervisor



DOH Mandatory Training FY2013-2014

The Local IT Disaster Recovery Coordinator is responsible for planning and directing the detailed information technology activities before, during and after a disaster on a local level. The Local IT Disaster Recovery Coordinator also ensures the implementation of the local Continuity of Operations for Information Technology Plans also known as the COOP-IT Plans.

The Continuity of Operations Plans, or COOP, or COOP-IT, are the plans designed to set standards for disaster preparedness. If you are involved in the Continuity of Operations Plan for your division, program area, CHD or CMS area office, be familiar with your responsibilities and make sure you can maintain the confidentiality of records during activation of the plan. Be sure to review and test the plan annually.


If you have any questions regarding your local COOP procedures, contact your supervisor.



Slide 23 – Information Resource Management Security Section

Information Resource Management Security Section

- Addresses confidentiality, integrity & availability of DOH information technology (IT) resources
- Department networks remain available & secure
- Only approved hardware & software permitted
- IT security responsible for processes, devices & software to implement security
- Access to data & information systems is on a “need-to-know” basis
- Proper security controls should be conducted



DOH Mandatory Training FY2013-2014

The Information Resource Management Security section addresses the confidentiality, integrity, and availability of DOH information technology, or IT, resources. Department IT resources and their security are critical.


As a member of the DOH workforce, you should be aware of the following key points:

- Department networks must remain available and secure
- Only approved hardware and software are permitted on DOH networks
- IT security is responsible for network processes, devices and software to implement security
- Access to data and information systems are on a “need-to-know” basis and
- Proper security controls should be implemented

Slide 24 – Have Questions?


Have Questions?

DOH Division of Information Technology



Information Security Manager:
phone (850) 245-4687

Information Security Intranet Page:
<http://dohiws.doh.ad.state.fl.us/Divisions/IRM/index.htm>



DOH Mandatory Training FY2013-2014

If you have any questions about this training or would like more information regarding the Department’s information security and privacy policies, please contact the Division of Information Technology, Information Security Manager, via phone at (850) 245-4687, or visit the Information Technology intranet web page at

<http://dohiws.doh.ad.state.fl.us/Divisions/IRM/index.htm>.






Slide 25 – End Slide

DOH Mandatory Training FY2013-2014

End of Information Security & Privacy Awareness Training Section 3

Return to the course & take the post-assessment



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

This concludes Section 3 of Information Security and Privacy Awareness Training. This is the final presentation for this course. Please return to the course and take the post-assessment.

END

