

Information Security

Level 1

TRAINING FOR ALL EMPLOYEES OF THE FLORIDA DEPARTMENT OF HEALTH





Acknowledgments

We would like to thank all of the workgroup members and other Department of Health staff that contributed to the development of the Information Security Level I Module. This instructional package was developed collaboratively from the efforts of the following work group members:

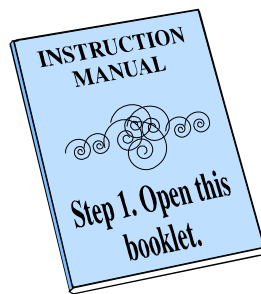
Drew Adams
Karen Hastings
Marilyn Houston
Darlina Hubbard
Robert Lester
Marilyn Maud
Linda Pearce
Jackie Seabrooks
Sandra Schoenfisch
Chris R. Smith
Rhonda White
Nancy Knox
Gail Harper
Vince Vaughn

A special thanks goes to those content experts who played a key role in the design and development by providing invaluable insight, critique, suggestions, and revisions. Their efforts were beyond the call of duty and imperative to the success of this project. They are:

Marilyn Houston-Palm Beach County Health Department
Darlina Hubbard-Pinellas County Health Department
Nancy Knox-Children's Medical Services
Chris Smith-Monroe County Health Department
Rhonda White-Information Resource Management Office

PURPOSE OF THIS MODULE

The purpose of this module is to ensure that all employees of the Florida Department of Health fully understand the Department's Information Security Policies, Protocols, and Procedures. This purpose will be accomplished by completing this module, by further independent review in the future, and by attending any accompanying training session(s) offered by your Department of Health division, office, county health department, Children's Medical Services clinic, or the A.G. Holley Hospital.



Why do I need this training?

First of all, the Department of Health views you as a valuable asset. We recognize that you bring unique and competent skills to the Department of Health. This training is to help you develop an awareness and a concern for information security to complement your skills as you serve the public of Florida.

Secondly, all new Department of Health employees and volunteers are required to receive security awareness training within 30 days of employment. Access to confidential information is not permitted until this training is completed. All employees must also complete security awareness update training once a year.

Each Department of Health division or office has the option of using this training module as a tool for self-paced learning or as a part of a group-lecture. Please complete the module and optional pre/post test as directed by your supervisor or trainer. At the end of the instruction, be sure to sign the confidentiality agreement and return it to your supervisor.

COURSE OBJECTIVES



At the end of this training you will be able to:

I Overview

1. Define “information security,” describe why it is necessary, and how it relates to your job.
2. Identify who is responsible for information security.

II Roles & Responsibilities

3. Identify the roles and positions established to help you safeguard information.
4. Explain how as a team member you safeguard information.

III Sharing Information

5. Define which information is considered confidential and needs security.
6. Define what it is meant by having a “Need to know”.
7. Identify the criterion for “Authorized Staff” and identify required authorization during the following activities:
 - a. access to information
 - b. update information
 - c. release of information
8. Describe the different types of information requests the department receives and who is authorized to release each type.

IV Maintaining Confidentiality

9. Appropriately and effectively maintain confidentiality as it pertains to clinic and field operations.
10. Utilize appropriate business practices and technologies such as:
 - a. Billing
 - b. Telephones
 - c. Fax machines
 - d. Computers

V Risk Awareness

11. Explain what to do if you suspect a breach of security or confidentiality or violation of policy & procedures.
12. Appropriately report incidents.
13. Describe the key motives for such incidents.



Introduction

Information Security is an Inside Job

The goal of this training is to make you more aware of the need for information security. This module presents the core issues in safeguarding information that are relevant to all employees of the Department of Health. Keep in mind that there is no such thing as absolute security. Training alone can not provide you with the solutions to every situation you will encounter. We expect this training will help you to become "security conscious" and able to spot "risky" situations, avoid potential security breaches, and help your fellow Department of Health employees to safeguard information.

Without your help, the Department of Health cannot keep information secure. Since every situation that may arise will not be included in this training, all we can expect is your commitment to follow and maintain policies and procedures for information security by following the guidelines in this training, the direction of your supervisor, and your own common sense. Remember that information security is an "inside job".

The Scenarios

This module presents scenarios introducing and concluding each section. The scenario at the beginning of the section will illustrate a situation where improvement is needed in order to safeguard information. The concluding scenario will present a similar situation illustrating the same principles for safeguarding information performed correctly. The scenarios attempt to give illustration to the concepts and principles found within the corresponding section.

THE NAMES AND CHARACTERS WITHIN THE SCENARIOS ARE FICTITIOUS. ANY RELATION BETWEEN SCENARIO CHARACTERS AND ANY REAL DEPARTMENTAL EMPLOYEES ARE PURELY COINCIDENTAL.



SECTION I *Overview of Information Security*



Hazard Clinics Story

It was eight minutes past the end of Gwen's shift as receptionist for Hazard Clinic. The day had been very busy, and all Gwen wanted to do was go home. Phil, the evening receptionist was a little late and Gwen was waiting for him to arrive so she could go home. Gwen's thirteen year-old son Dale, was waiting with her.

"Mom, can we go now?," Dale asked.

"Phil should be here any minute, Dale. We can go then, okay? At that moment she noticed Phil's car out in the parking lot. It was dark out, but she knew Phil's car well. Gwen squinted to get a better focus. Despite the darkness, she could tell that Phil wasn't in the car. She became concerned, wondering if Phil was okay.

"Dale, sit here behind the counter and don't touch anything until I get back. I'm going outside for a minute." Gwen went out into the parking lot to see if she could find Phil, while leaving the front office area of Hazard Clinic all alone except for thirteen year old Dale. Dale plopped down on Gwen's chair and spun around a few times. When the spinning chair stopped, Dale looked up at Gwen's computer screen. Across the screen were names, addresses, and phone numbers of what must have been clients of the Department. *Whoa*, Dale thought. He scrolled through a few names and read with interest all of the information in front of him.

"Holy cow," Dale whispered in amazement. He recognized one of the client's addresses as a street within his own neighborhood. *Oh my goodness, I think I know where that house is*, Dale thought.

Just then both Gwen and Phil walked in, talking. Dale jumped up from his seat, realizing that maybe he was looking at something he shouldn't have been.

"Sorry you two were waiting on me," Phil said. "I was trying to fix my taillight on my car real quick before coming in and I must have lost track of time."

"No problem," said Gwen. "We're just glad you're okay. Dale, are you ready to go?"

“To promote and protect the health and safety of all residents and visitors.”

--The Mission of the Department of Health

The Florida Department of Health provides valuable services to the residents and visitors of Florida. We refer to the people that we serve as our clients. A crucial element in providing health services to our clients is information. The collection, maintenance, and dissemination of information is critical to achieving the mission of the department. Securing this information is a priority.

Think for a minute of how your bank or credit union provides financial services to you and many others in your community. A bank's product is quality financial services. Money is a major vehicle in providing this product. At the Department of Health, our product is quality health services. A vital element in producing this product is accurate and reliable information. Therefore, secure information is our business at the Department of Health.

Why do we safeguard information?

The Florida Department of Health requires a solid foundation of trustworthiness. The community must trust us to provide quality services, protect their health interests, and be a source of valid information. The collection of information is essential to our efforts. Sharing information is also an obligation in certain instances. Many aspects of our mission involve confidential information, and in these areas, it is essential that we protect all clients' confidentiality and right to privacy. If this trust is compromised, we will be unable to perform our mission.



The obligation for protecting this information is both moral and legal. Federal and state laws require that all health care facilities adhere to strict security policies and procedures in order to keep information secure.

Information security is a method to protect information and ensure:

- **Data integrity is maintained**
- **Appropriate access to the information**
- **Confidentiality is maintained**

Throughout the nation, policies and procedures are being established to accomplish these goals. In order to standardize the practices which safeguard information, the Department of Health has recently published a document entitled: "INFORMATION SECURITY: POLICIES, PROTOCOLS AND PROCEDURES." The policies document proactive steps to help you, as a Department employee, safeguard information. Although it seems that common sense would tell us how and why we must keep information safe, you will see that it can be easier than you think to handle information inappropriately.

Consider the following scenario:

A nurse received a phone call from a city police officer requesting medical records on a client. He specifically wanted the results of HIV, Hepatitis A, B, and C tests, which were recently performed. During the conversation, the police officer told the nurse that the Client confirmed that s/he had recently been seen at the clinic and had received these tests. The police officer was calling to confirm information provided to him by the client. During their conversation, the nurse did confirm that the client had been seen recently and did have tests performed, but the nurse did not actually state what the tests were. Following this incident the nurse received a written reprimand.

Why did the clinic determine this was a violation of confidentiality despite the nurse's efforts to safeguard information?

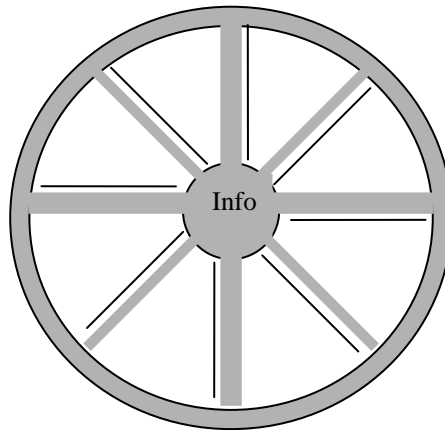
As you can see, this is a very serious matter that can prevent us from providing quality health services without the active concern of every Department of Health employee, volunteer, and contractor.

Who is responsible for information security?

You are. All employees and volunteers of the Department of Health who have access to any information are required to preserve the integrity of the data and handle it in such a way that keeps it safe. Information within the Department of Health progresses through and can be found in three different phases: *Collection*, *Maintenance*, and *Dissemination*. Information is first collected through a variety of sources. Then information is maintained in a variety of records and files. And finally, information is disseminated or shared as necessary.

Think of this process like a wheel. (See figure 1)

figure 1



The rim of the wheel represents health needs and services and the point of entry for data collection or receipt. The rim also serves as the transport vehicle to move information from one point to another.

Consequently, the hub of the wheel represents the storage and maintenance of the information. It is housed within the center of the wheel, the most secure area and highest level of protection from external forces.

The wheel's spokes represent the flows of information as it enters and exits the Department of Health. This is where the *collection* and *dissemination* of information occurs. The spokes also represent departments or divisions that may need the information.

Information may travel from many different sources and may be needed simultaneously by several programs, departments or divisions. Information travels from one spoke to another via the rim of the wheel.

To illustrate, consider the following example.

Melissa Hansen is a college student who suspects she may be pregnant. She decides to visit the county health department in her community for an examination. At the health department she is examined by the physician and a nurse. Before the actual examination, however, Melissa filled out a questionnaire concerning her medical history. During the examination, it was discovered that Melissa was indeed pregnant. Melissa was then referred to an OB/GYN outside of the health department. All of this information was put into her medical record.

As you can see, in the information process, Melissa is a member of the community who has a health need. Her needs are included in the rim of the wheel. As the clinic receptionist, nurses, and physician collect her information, it flows into the Department of Health by following the spokes of the wheel. Finally, the information is stored securely in the hub of the wheel where it will be maintained. When Melissa is referred to a community OB/GYN physician, her medical information is released to that physician's office. Thus, the information is then disseminated along the spokes of the wheel as it leaves the Department of Health.



Remember that information is what allows the Department to provide quality health services to the citizens of Florida. To do that, information must be collected accurately, maintained securely, and disseminated properly.

Just like a car could not get anywhere without its wheels, the Department of Health could not provide health services without this information process wheel working effectively. Although there are many different roles and positions within the Department, we all share the responsibility of safeguarding information. It is regardless of whether your position requires you to collect information, maintain information, or disseminate information, or a combination of all three, you must do your part to keep information safe.

Section I Review

Competent Clinic's Story

Latisha was the front desk receptionist at Competent Clinic. It was Wednesday, the day Latisha had a final exam in her English class at the local community college. She was scheduled to get off at noon which would give her just enough time to fight traffic to get to school, get a good seat, and review her notes one more time before the exam. There was only one problem, however. It was five until noon and Ben and Paula, the other receptionists were not back from eating lunch at the cafe next door. Ben and Paula had agreed that they would be back in time to relieve Latisha by 11:45. Latisha was getting nervous.

Since the cafe was just next door, Latisha thought that if she walked out to the parking lot and waved at Ben and Paula, she'd get their attention so she could leave. This of course meant leaving the desk alone. Since there was no one in the office except for Mr. Reynolds, the janitor, leaving the desk would have minimal consequences.

Latisha scanned her desk to make sure no confidential information was insecure or exposed. None was. Then she looked at her computer screen and noticed that the client database was on the screen. Though Mr. Reynolds was a competent employee and was someone who she thought could be trusted, Latisha made sure she logged off of the computer so that no information was in the screen at all. It would require a password to get back on. She made certain that all information was safeguarded before leaving her desk. She could now go and flag Ben and Paula. Before she did so however, she stopped and thought that she should reconsider her leaving the desk alone. *I'm just going to have to wait*, she thought, knowing that leaving the desk would be inappropriate.

Just then Ben and Paula came storming into the office with apologies about being late; they had completely forgotten about Latisha's test.

"No problem," Latisha good-naturedly reported, and left to go take the test.

What may have happened had Latisha not taken these steps to safeguard information?

What did Latisha do in order to safeguard information that was different from Gwen's (from Hazard Clinic) actions?



Section I Review Questions

Please answer and discuss the following questions with your trainer/supervisor as needed.

1. As a healthcare worker, you have an ethical responsibility to keep client information confidential.

True False

2. If clients don't trust healthcare workers to protect their confidentiality, they may not seek the care they need.

True False

3. Failing to protect client privacy may cause a little embarrassment, but no real harm.

True False



SECTION II

Roles & Responsibilities

Hazard Clinic's Story

Dave had just started as a nurse at the Hazard Clinic. From previous experience, Dave knew how to be a good nurse, but there were some things that he felt he needed to brush up on. Dave's supervisor Ken, kept mentioning some training that he would receive sometime in the future as soon as they found the time. Dave made himself available on several occasions but it always seemed like Ken was too busy and would never establish a date with Dave to provide the training. Nevertheless Dave went about doing his job as best he could.

One afternoon however, some things happened that made Dave wish he had received that training. Dave was in the middle of examining a six year old boy when an emergency phone call came in asking specifically for Dave. The receptionist interrupted Dave and the client to give him the message.

"It's an emergency?," asked Dave, looking up from the client's medical file.

"Yes. The person on the line said it couldn't wait."

"Huh, all right." Dave looked at his patient and put the file down on the counter next to the little boy, and said: "We were almost done here anyways, weren't we, Big Guy?"

"Yeah," the little boy said happily. Dave left the file with the boy and left to answer the phone.

Dave was on the phone for only a few minutes, and immediately returned to the examination room only to find his little patient was gone. Dave looked up and down the hall and then jogged into the front office to see if he or his parents were there. As he looked out the front window, he saw the little boy and his father get in their car and drive away. Dave also noticed that the boy was holding the medical record.

"Where are they going?" Dave asked. "His examination isn't over and he's leaving with the medical record."

"They left?," The receptionist asked. "I didn't even notice, due to the office being so crowded."

"He must have assumed the examination was over when I left for the phone," Dave guessed. "I Left the file with the little boy for just a minute, and he must have thought it was something he was supposed to keep."

"We'll have to give them a call to get those records back," the receptionist said. "We don't want those getting in the wrong hands."

We're a team!



Just like successful sports teams must have individual players with specific jobs that work together as a whole, the Department of Health has established specific roles that work together to safeguard information. The team members that play a key part in safeguarding information include your Administrator/Director, Security Coordinator, Information Custodian, and your supervisor. In your efforts to keep information secure, you will receive plenty of help, training, and guidance from each of these people. The specific information security responsibilities of each team member are listed below.

Director/Administrator

As the title implies, the director's primary role is to manage a specific Department of Health location. Part of this role includes the ultimate responsibility for all activities of his unit including information security. To assist in this function, the director appoints a Security Coordinator and a group of Information Custodians to effectively coordinate the local information security activities.

Security Coordinator

The Security Coordinator coordinates the security activities at your department location by:

- disseminating the information security policies, protocols, and procedures in whole or in part to staff, based on a need to know.
- ensuring that formal security awareness training is available within:
 - the first thirty days of every new employee's employment and
 - annually to all employees.
- monitoring adherence to the protocols and procedures for secured
 - areas and coordinating corrective action as appropriate.
- supporting the information custodians to maintain appropriate
 - security of each information set.

Information Custodian

To make the information security efforts more manageable for each team member, information is categorized into groups of information with similar characteristics called *information sets*. You may come in contact with various sets of information throughout the course of your day.

Information Custodians are Department employees who are responsible for taking measures to secure specific information sets. Information custodians act as “gatekeepers” to information sets within your Department of Health location by allowing access to only those with a need to know. Every set of information within the Department of Health has an information custodian assigned to it.

Supervisor

Your supervisor will help you to safeguard information by informing you of the information sets that you may encounter and of the custodians responsible for those sets. Also, he or she will establish performance standards that are relevant to your specific job duties, including directions on how to keep information secure. Your supervisor will communicate these standards to you, as well as provide job specific training relating to specific information sets within the scope of your duties.

Individual Employee

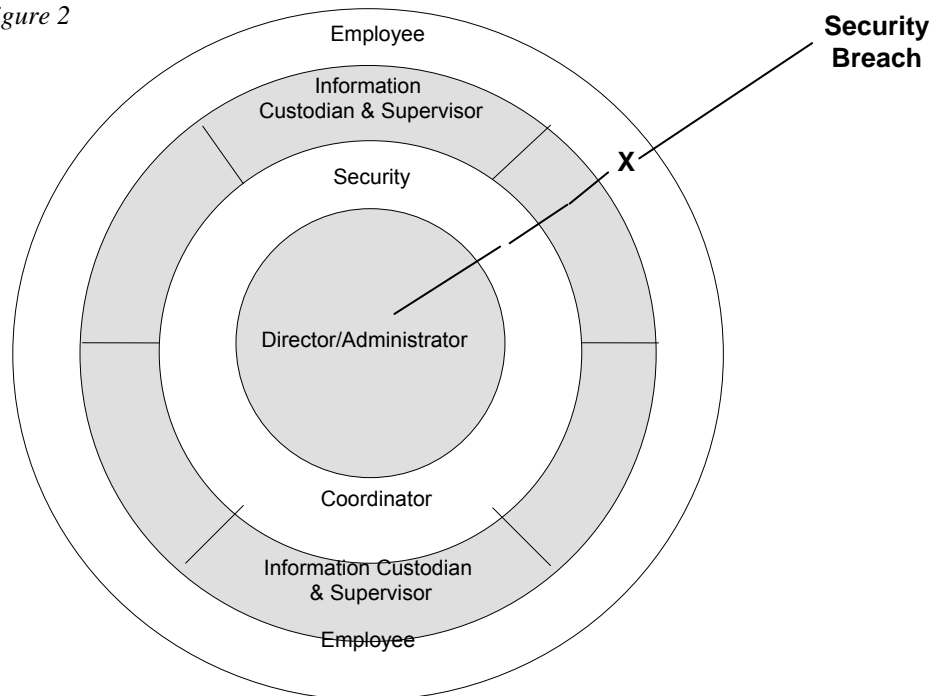
Every individual employee is an important team member in the process of securing information. Without your commitment, all the efforts of the Director/Administrator, Security Coordinator, and Information Custodian and supervisor would be futile.



As stated in the previous section, everyone within the Department of Health is required to safeguard information for the purposes of maintaining data integrity, appropriate access and confidentiality. We act as a team by helping each other to protect information. Without the help from each team member, it would be difficult for every employee to know how to safeguard information in every situation. This means we all share a responsibility for information security. If a breach occurs, it may have been avoided with the help of the team members we have discussed. If this is the case, accountability for the breach is then shared by all team members involved. Ultimately, however, your Director/Administrator is responsible for the information security at your Department of Health location.

Figure 2 below illustrates the level of responsibility by role as well as demonstrates the accountability in the event of a security breach.

figure 2





As you can see, at the Department of Health, securing information is a team effort. For example, if a receptionist in your clinic/office calls a sixteen year old client to remind her of her follow-up family planning appointment” and decides to leave that particular message with her mother (who had no idea her daughter was a client of the department), a breach has occurred. Who’s accountable? Consider it a loss that the team suffers. It is clear the receptionist “dropped the ball” by revealing confidential information to the girl’s mother, but there may be more to the story. It is possible that the receptionist’s supervisor and/or information custodian had not clearly defined how to properly remind clients of their appointments. Perhaps the security coordinator had not ensured that the receptionist had received training on Information Security. In these situations, the receptionist’s breach may have been avoided had each team member carried out their responsibilities more effectively.

Section II Review

Competent Clinic's Story

Chuck, the nursing supervisor hung up the phone and smiled at the application and resume that sat in front of him on his desk. He had just called Angela Hatfield to let her know that she got the job as the new nurse at Competent Clinic. Chuck was pleased and optimistic about Angela. She had been a pediatric nurse at the local city hospital for four years until being laid off due to heavy cut-backs. He glanced again at the list of accomplishments on her resume. This was Chuck's favorite section. *Employee of the Month*, was the item that particularly had a nice ring to it.

As Chuck reread the resume, Michelle Geurra, Competent Clinic's security Coordinator walked by outside Chuck's door.

"Hey Michelle, come check this out!"

Michelle stopped and leaned inside the doorway of Chuck's office. "What is it, Chuck?"

"Our new ace nurse. Look at her qualifications, will you?" Chuck beamed as he handed Michelle the resume.

Michelle studied the resume. "Very nice, she should make a great staff member. When does she start?"

"Monday, which is perfect because Lucille won't be back from her daughter's wedding yet. I wasn't sure who would fill her shift, but now I figure Angela could start Monday afternoon after orientation," Chuck said as he waved Angela's application in the air for an emphasis of joy.

"Hold on there, big shot. You don't think she'll be seeing any clients before she receives her information security training do you?"

"That's the best part, Michelle. She doesn't need the information security training. She's experienced."

"Chuck, regardless of experience, all employees of the Florida Department of Health must receive mandatory information security training or they will not be granted access to confidential information, and as a Nurse, I have the feeling handling confidential information is a part of her job. Wouldn't you agree?" Maria asked.

"Yeah, yeah, you're right," Chuck agreed.

"It's policy, Chuck. And besides, we're a team here at Competent Clinic. We help each other out. You and I will do our part to make sure Angela knows how to safeguard information. Maybe we could schedule her training after orientation on Monday afternoon. Does that sound good?"

"Yep, sure thing." Chuck answered scribbling in his planner.

What was done different in Competent Clinic than in Hazard Clinic?

Who was responsible for the breach in Hazard Clinic?



Section II Review Questions

Please answer and discuss the following questions with your trainer/supervisor as needed.

1. It's your responsibility alone to become familiar with Department policies and procedures on client confidentiality and follow them.
 True False
2. All Department of Health employees must receive information security training within the first ninety days of employment.
 True False
3. The training that you will receive will show you how to respond in every situation that you will encounter as an employee of the Department of Health.
 True False
4. Because they are not paid employees, healthcare volunteers are exempt from confidentiality requirements.
 True False



Section III

Sharing Information

Hazard Clinic's Story

Zack, an STD case manager of the Hazard Clinic walked one his favorite clients, nineteen year-old Pat, to the door. Pat had just had his first visit to see the doctor after discovering that one of his previous sexual contacts had an STD. Zack, through his interviews, had been the one to inform him that he may be at risk.

"Take care, and be sure to do what the doctor says, okay?" Zack said as Pat walked out the door. Pat waved back at Zack and then walked to his car. Zack walked back to the receptionist area where the receptionist was busy filing some papers.

"Will you let me know if you hear anything I should know about for Pat's case?" Zack asked the receptionist.

"Yeah, sure," the receptionist answered.

A couple of weeks later, Zack found in his box a memo from a health insurance company. The memo was a request for medical information on Pat. *Why is this in **my** box, of all people? This should be in Medical Records, Zack thought. Oh well, no problem, I'll help Pat out.*

Zack got Pat's file to make sure there was a release from Pat authorizing third party payers to receive his information. He couldn't find one. Zack assumed either Pat forgot to fill one out as he seemed upset the other day or maybe it was misplaced. Why would he have health insurance and not allow them to pay for his medical costs? So Zack felt like something of a hero as he faxed Pat's medical records to the insurance company so that they could pay for his medical services.

When Zack got back to his desk he called the receptionist to report that he got the memo that was forwarded to him and that he saved the day.

"You did what?" The receptionist gasped.

"I faxed Pat's information to his insurance company for him, like I said. Why, what's up?"

"Pat never signed a release. He probably didn't want his insurance company to receive the information because that's probably his parent's insurance policy and they could get the bill. I forwarded the copy of the request to you because I thought you might need it for your case" the receptionist explained

"Oh." Zack suddenly didn't feel very good, at least nothing at all like a hero.

What information is considered confidential?

In the Department of Health, there are basically two types of information: public information and confidential information. The difference between the two are explained below.

Confidential Information

Confidential information can be defined as information intended to be kept private. Confidential information identifies an individual with medical or psychiatric information, such as diagnosis or treatment, financial or social information. This information is protected by Title X of the U.S. code and the Florida Sunshine Law. Examples of confidential information include birth certificates, medical records, or any information that may identify a person as a client of the Department of Health.

Public Information

Public Information can be defined as any information that a person can acquire by invoking Title X of the U. S. Code or the Florida Sunshine Law. Basically, it is information that can be accessed or shared by members of the community. Although the interested person may have to do some digging and probing to get it, the information is not confidential. Examples of public information includes death certificates (excluding cause of death), e-mail, Department of Health salaries, reportable disease statistics, etc.

Both confidential and public information must be safeguarded. Since the inappropriate release of confidential information has more serious consequences than releasing public information, the department limits access to confidential information to staff with a documented "need to know."

What does it mean to have a “need to know?”

Need to Know - a condition when an employee must have access to specific information to perform the routine duties of the job and provide services to the patient or community. The job duties define the “need to know”, not the individual. Every person sharing those duties would have the same “need to know”.

If you absolutely cannot perform your job as defined in your position description without access to a specific set of confidential information, then you have a “need to know.” Your Security Coordinator, Information Custodian(s), and supervisor implement procedures to ensure that persons with a “need to know” information have access to such information and restrict access to all others. “Need to know” for an individual employee or volunteer will be established by the director and documented in that individual’s position description and performance standards. This is what is meant by a *documented* need to know. If this “need to know” is not documented in your position description, then you will be restricted from access to information sets. There are very few people who will have access to all information sets within the work setting.

Employees of the Department of Health, can be authorized to share information in three ways:

1. Authorized to have access to information
2. Authorized to add to, update or change information
3. Authorized to release information

Your position description should be specific as to what information you are authorized to have access to and/or release. If your position description leaves you uncertain about your authorization, please see your supervisor for further clarification.

Why would anyone want our information?

Many times, in order for the Department to adequately provide quality public health services, parties inside and outside of the Department of Health need access to certain confidential information. Examples of these outside parties include the client, health insurance companies, other physicians, specialists, or attorneys. Information requests generally fall into four categories:

1. Continuity of Care Requests
2. Subpoenas and Court Orders
3. Personal
4. Third Party Payers

Continuity of Care

Frequently information needs to be shared to provide continual quality care for our clients. For this to be possible, a continuity of care request must be received from those health care providers who need information from the Department of Health in order to serve the client. Continuity of Care Requests include requests for information from outside health care providers or facilities that need our information to provide health care services to our clients.

Subpoenas and Court Orders

Occasionally confidential information within the Department of Health is needed in legal matters such as lawsuits, disputes, or client and community protection. In these situations, the requesting parties must have a subpoena or a court order to obtain the information. A subpoena is a legal document requiring an individual to appear in court to give testimony or provide information to the court in lieu of personal appearance. A court order is also a legal document that is issued by a judge. Procedures for accepting and processing subpoenas or court orders will be established and shared with you if your duties will involve the receipt of these documents. Information will be provided to you by your supervisor.



Personal

Clients may request their medical information be sent to other parties that are not represented by the health care system or the legal profession. The patient may authorize anyone to receive their personal medical information and this request must be honored. The most frequent requests we see are for insurance applications, Social Security disability claims or family members. However, any individual can be authorized to review the medical information based on the client's desire and written statement authorizing the review.

Third Party Payers

Many clients have arranged to have a third party pay for the services they receive at the Department of Health. These third party payers include health insurance companies, health maintenance organizations, Medicare, Medicaid, etc. To be able to effectively render these services to the client, the third party must have access to the information concerning the client's treatment at the Department of Health. In order to release information to a third party payer there must be a request on file with the Department of Health that includes the client's authorization to release information to that specific third party.

There are various reasons why information is requested from the Department of Health. Listed above are the categories in which most requests would be found. If your position description includes the responsibility of releasing information, your supervisor and information custodian will train you on the specific conditions and requirements of each information request type.

When can information be released?

The circumstances which allow information to be released from the Department of Health is largely contingent on what type of information is being requested. As mentioned earlier, the Department of Health works with two basic types of information: confidential and public. Both types require certain conditions to be met for release.

Confidential

Requests for confidential information must be very explicit about identification, authorization, purpose, and intent. The request must at least include:

- the name of the party requesting the information
- authorization from the client
- dates of the authorization and the request
- client identification
- the purpose for which the information will be used
- extent of information to be released
- a statement that the consent can be revoked

These conditions are common requirements in most requests, however, different circumstances warrant different conditions. Your supervisor will help you to know the appropriate requirements for the requests that you might receive.

Public

Requests for public information are similar to confidential although the constraints are much more relaxed. The request must specifically include the name of the party requesting the information as well as the extent of information to be released.

Remember-

A good rule of thumb is to contact your information custodian or supervisor anytime you receive a request for information and are unsure about how to handle it appropriately. If they are unavailable or unable to help you, and you are unsure about what to do, **DO NOT RELEASE THE INFORMATION UNTIL YOU CAN CONSULT WITH THE APPROPRIATE INFORMATION CUSTODIAN.** It is better to be safe than sorry.



SECTION III REVIEW

Competent Clinic's Story

Katie Strachan had been a case manager for six years at the Competent Clinic. She'd pretty much seen it all, she thought. Things had smoothed out to being routine by her third year on the job, and now after being there even three more years, she felt she could do her job in her sleep. That's why when she had to attend annual information security training last month, she felt she could've lip-synched the whole presentation. What she didn't realize however, was that the review would save her from a tight spot one morning the following week.

Katie was in the break room enjoying a bagel before her next client when Angela, the new nurse came in to tell her that she had a visitor out front.

Katie walked out to the front desk area where a professionally dressed woman was waiting.

"Hi, I'm Katie Strachan, can I help you with something?"

"Yes," the woman said politely. "I'm an attorney representing a case that involves your client, Joseph Stoltz." She paused waiting for Katie's reply. "When did you last see Joseph on a medical basis Ms. Strachan?"

Katie thought about it. Joseph had come in either last Wednesday or maybe Thursday for a check up. Katie was about to answer the woman, when she remembered something from her training the week before: "*Confidential information identifies an individual with medical or psychiatric information, such as diagnosis or treatment, financial or social information.*"

"I'm sorry. If we had such records, Florida statutes would prohibit me from disclosing them to you without the written authorization of the person to whom they pertain," Katie said, making sure not to acknowledge that Joseph was a client.

"Ms. Strachan, we have reason to believe that Joseph is a patient here and as an attorney representing an important case, I am trying to help Joseph by gathering all relevant facts," the attorney said genuinely.

"I'm sorry, but even if this person was a client here, you'd have to have their written authorization indicating that you could receive any information. Unfortunately, I can't help you until you produce such authorization." Katie responded politely.

"I understand. Thank you for your time anyway." The attorney smiled and left.

What was the difference between Katie's and Zack's (from Hazard Clinic) efforts to safeguard information?

What could have been done differently at Hazard Clinic?



Section III Review Questions

Please answer and discuss the following questions with your trainer/supervisor as needed.

1. Confidential information may include information about a client's financial situation.
 True False

2. A client's healthcare information should be accessible only to those who "need to know" it to deliver care to that client.
 True False

3. Members of a client's immediate family should always be given access to the client's records.
 True False

4. For convenience, medical records should always be kept at the foot of the client's bed.
 True False

5. Client information must always be written to be considered confidential.
 True False



Section IV

Maintaining Confidentiality

Hazard Clinic's Story

Denise, the Dental Assistant at the Hazard Clinic, was busy sterilizing the instruments Dr. Michaels had just used in the prior exam. The next appointment wasn't for another half hour, so she decided to go to the break room and get a snack. Doug, a health technician was sitting at one of the small tables in the break room eating his lunch when Denise arrived. A young woman that Denise didn't recognize was purchasing a soft drink from the drink machine. Denise waved at Doug, and then pumped a few quarters in the snack machine and made her selection. The young woman left.

"So, what's new, Denise?" Doug asked, chewing his sandwich.

"Not much. Same old stuff, I guess." Denise sat down on the counter to eat her candy bar.

"Have you had a lot of clients today?"

"Nope, just one. That big blonde guy, did you see him?" Denise asked Doug.

"Uh, yeah. I think that was his girlfriend that was just in here getting a drink."

"All I can say is, thank goodness for rubber gloves," Denise said, shaking her head.

"Why, what do you mean?" Doug asked.

"Well, he had hepatitis B and dental clients of course always bleed. You just really have to be careful."

"Yep that's for sure. Everyone needs dental care though. Hey, you want my orange? I'm full." Doug was holding his orange towards Denise.

Just outside the doorway to the break room, the girl that had bought the soft drink had been leaning up against the wall drinking her soda, waiting for her boyfriend who was in the bathroom following his dental exam. Denise and Doug's conversation had been very clear in the hallway.

He's got Hepatitis B! , the girl was thinking. What am I going to do?

What about general day-to-day business practices? How can I help to maintain confidentiality then?

This section will focus on the steps we take to safeguard confidential information by addressing three areas:

- Maintaining Confidentiality in the Clinic/Office
- Maintaining Confidentiality in the Field
- Maintaining Confidentiality while using Business Technology

Maintaining Confidentiality of Clinical Information

Secured Areas

Remember learning about employees with a “need to know?” By identifying information sets and documenting who has a need to know the information found within the sets, we take the first steps in protecting information. To further ensure that this information doesn’t get into the wrong hands, secured areas have been designated throughout the Department of Health.

A secured area is an area with a reliable locking system, including a dead-bolt lock with access limited to a documented list of authorized personnel. The doors will be securely locked at all times when no one is in the secured area. The secured area has access limited to a documented list of authorized personnel. Personnel are designated by their position and will be authorized based on their need to know. Also, if personnel not on the authorized list need to visit the secured area such as technicians, support staff, or senior management, an access log is kept for them to record their visit and the reason for the visit. Persons with temporary or occasional authorized access must be escorted at all times while in the secured area.

Handling of Medical Records and Other Confidential Client Identifying Information

- Records that are pulled for an upcoming appointment or are awaiting re-filing are to be in a secure area with visibility and access limited to authorized personnel only.
- Confidential information should never be left where clients can see or read it. This includes unattended rooms with open doorways.
- When documents that contain links to client names and services must be destroyed, they should be shredded rather than thrown into the wastebasket. Wastebaskets can be a great source of information.
- The exterior cover of a medical record must never identify sensitive information, nor shall records be stored in a manner that would distinguish them from any other record, for example, HIV positive clients' charts must not be segregated due to their special status.

Discussion of Client Information

- Information discussed by health team members in conferences or team meetings must be held in strict confidence. Never engage in discussions of confidential information in public areas within department locations such as hallways, elevators, rooms with open doors, rest rooms, etc.



- Information discussed by health team members must be limited to only those with a need to know.
- Discussions about clients and employees must be limited to information necessary to provide care or perform job functions.

Billing Procedures

Although your supervisor will train you on the specifics of how to handle the specifics of billing procedures, there is some general guidance that is relevant to this training.

- Remember that billing documents usually link client names with services and therefore are confidential information and should be treated as such.



- Clients must sign a third party release form authorizing the Department of Health to release their information to the third party.

Maintaining Confidentiality in the Field

Personnel frequently must leave Department offices and go out in to the community (the field) in order to provide services to clients. Sometimes this requires removing confidential information from the secured area. One can easily imagine how this type of service delivery puts confidential information at risk. In order to ensure confidentiality in the field, the following efforts must be made:

- Confidential information must be taken into the field *only* by those persons who *absolutely* must have the information in order to perform field investigations, such as home visits, visits to off site clinics, etc.
- Personnel must only take information into the field that is relevant to those clients they will see that day.
- All efforts must be made to minimize the amount of data that is transported in to the field.
- Client information used or obtained in the field must be safeguarded from access by unauthorized personnel, and must never be left unattended. All information must be secured in its designated area by the close of business each day unless prior authorization has been given.

How to Maintain Confidentiality While Using Business Technology

With the speed of new business technologies comes the greater potential for effective and efficient communication. Examples of communication technologies that we use in the Department of Health are telephones, photocopy machines, fax machines, and computers. We use these technologies in virtually all of our day-to-day business activities such as inter-office communication, billing practices, data storing, etc. Unfortunately, these technologies present a risk for breaches if not handled properly. The following discussion addresses how to properly use the phone, fax machines, computers.

How to Maintain Confidentiality While Using the Phone

- All telephone calls should be answered in a manner that does not identify clinic specialty or such designation that would compromise a client's confidentiality.
- Confidential information should never be released or discussed over the phone without verifying that the caller is legitimate.
- All telephone conversations in which confidential information is discussed must be made from an area that ensures that confidentiality is maintained.
- Appointment scheduling and appointment reminder procedures and documentation must be handled in a manner which ensures that client confidentiality is maintained.
- It is important to keep in mind that cellular telephones are not secure nor is the environment from which the call is made.



Remember:

By giving any information about a client's whereabouts or appointments to a person other than the client, you are, in effect, affirming that the person is a client. **This constitutes a breach of confidentiality.** Information of this nature should never be given to any person other than the client or the legal parent/guardian of a minor.

Using Fax Machines

By following these guidelines, you can reduce the risk of confidentiality breaches while faxing information.

- Only those employees with authority to release information can fax it to the requesting party. Again, this is determined by position and identified in job description.
- Fax machines that will receive or transmit confidential information must be maintained in a secure area
- When someone notifies you that they are sending a fax to your office, always ask if any confidential information will be included in the fax. If the message will include confidential information, give the sender the number to the fax machine that is maintained in a secure area.
- A cover sheet marked "Confidential" and containing the following paragraph must accompany all transmissions:

"This transmission may contain material that is CONFIDENTIAL under federal 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."
- The person receiving the fax has a responsibility to be at the fax and remove the fax from the machine immediately to limit access with others who might see the information.
- If a misdirected fax is received, the sender must be notified and the document must be destroyed.

Using Computers

Computers play a large role in the Department as they can be used for information collection, storage, retrieval, and processing. To increase your ability of maintaining confidentiality while using computers, follow the guidelines below. The guidelines are grouped into two categories: user access practices and physical security.

User Access Practices

- Access levels are assigned on a “need to know” basis.
- Each user has a unique user identification.
- Passwords should be eight characters or longer, should be changed every thirty days, and should never be disclosed.
- Screen savers are to be password protected as well.
- When exiting the system the employee should log off past all passwords, and not just walk away from terminal.
- Laptops containing confidential information must never be kept at an employee’s home and must be returned to the secured area at the end of the working day.
- Laptops are not to be used for storing or accessing HIV, AIDS, sexually transmitted disease and tuberculosis information with client identifiers.

Physical Security of Computers

- Monitors should be positioned in such a way that clients or others can not view the screen.
- Computer operation areas and network wiring closets should be maintained as a secure area. It is important to document all persons with temporary or occasional authorized access and to escort them at all times.
- Entrances to areas of highest sensitivity should be closely monitored.

Section IV Review

Competent Clinic's Story

Dr. Montrose had just finished seeing her patient, Todd Jackson, and had prescribed several procedures and tests to be conducted by the nursing staff. Dr. Montrose retreated back to her office to make a few calls when the office manager, Chris, came in to discuss some budgetary issues. In the middle of their discussion, Angela, one of the nursing staff, came in Dr. Montrose's office to ask a question.

"Dr. Montrose, I'm sorry to interrupt, but Todd and his family have some questions about his condition and his tests that we couldn't answer. Maybe you could help me with the questions, or would you prefer to speak with them yourself?" Angela asked.

"What are the questions, Angela?" Dr. Montrose asked, then shook her head. "Chris, could I discuss this with Angela alone? It won't take a minute."

"You bet. Let me know when you're free." Chris said, getting up.

"Thanks, Chris," Dr. Montrose said with a smile. "Now, Angela, will you shut the door and then we can discuss Todd's case."

How was the way Dr. Montrose handled the situation more effective than the way Denise handled it in Hazard Clinic?

Why did Dr. Montrose ask Chris to leave?

What else could have been done to maintain confidentiality in Hazard Clinic?



Section IV Review Questions

Please answer and discuss the following questions with your trainer/supervisor as needed.

1. Computerized healthcare information is confidential and should be treated like any other medical record.

True False

2. When off the job, you aren't required to keep client information confidential if you aren't acting in an official capacity.

True False

3. One of the easiest ways to safeguard healthcare information when releasing it is to fax it.

True False

4. When answering the telephone, it is best to be clear and avoid confusion by identifying clinic specialty (such as STD Clinic or HIV records).

True False



Section V

Risk Awareness



Hazard Clinic's Story

Over the past few weeks, Roger, a nutritionist at Hazard Clinic had noticed that Lorraine, one of the other nutritionists, had been faxing confidential information inappropriately. She had been faxing entire files instead of limiting the fax to only the needed information. Also, he noticed that she would send the faxes without notifying the receiving party that the information was confidential. Roger felt like he should do something about it so he decided to approach Lorraine. When doing so, however, she played it off like he was joking around. Roger couldn't tell if she was just laughing it off because she was embarrassed or maybe she really thought he was making a joke. He decided to let it go, feeling like he did his part to help her out.

The problem, however, was that she continued to make the same mistakes over the next couple of weeks. Since Roger felt like his last attempt to talk to Lorraine about the situation didn't work, he figured any further attempts would prove useless as well. He wondered if he ought to tell a supervisor about what Lorraine was doing, but then Lorraine might know it was Roger that had done the "tattle-tailing" since he had already spoken to her about it. Roger eventually just decided to not pay any attention to what Lorraine did since it was out of his control. He was just glad he knew how to fax confidential information correctly. Besides if there hadn't been any problems so far, it was quite likely there would never be any problems.

I understand that the Department of Health could not function without our safeguarding information. What can my fellow workers and I do to help each other keep information secure?

This training is one component of an information security awareness and breach prevention program within the Department of Health. Training alone, however, cannot cover every possible security issue that may arise. In fact, the entire information security program can effectively manage risk, but it does not eliminate it. There is no such thing as absolute security. With that idea in mind, this section intends to increase your risk awareness. Specifically, the goal is to increase your awareness of potential security breaches or hazards, to increase your awareness of how to prevent breaches by being more aware, and also to increase your intervention of potential or committed security breaches.

This section will address four areas:

- Suspected breach of confidentiality, security, and violation of Department policies and procedures
- Incident Reporting
- Things to look for (causes of suspected breaches and violations).
- Penalties that can be avoided by being risk aware.

Suspected Breaches & Violations

As employees of the Department of Health, we are all part of a team. As a team, we need help from each other to provide quality public health services. This means we need to all help each other to keep information secure. A safe driver drives cautiously and defensively, always on the look out for potential risks of accidents. Just like driving defensively in traffic, we need to always be aware of and on the look for information security risks. For example, you notice a nurse is examining a client's file when an emergency situation or some other distraction commands his/her attention and the nurse quickly puts down the file while running to help out. The client's file is left open for unauthorized access. What do you do? Do you gasp in disbelief and run to report the incident to the appropriate information custodian? Here's an idea: how about walking over to the file and close it? It also may be good to remind your fellow co-worker of the fact that they left the file open.

This is what is meant by risk awareness and by teamwork. We must always be sensitive to the fact that information must be secure. **A good way to develop risk awareness is to think of the information as if it held confidential information about yourself.** How would you want it to be handled? Each of us want our information to be protected when we go to our doctor and receive health services. Try to consciously handle each client's information as if it were your own. Viewing all information in this way will help you to be risk aware.

Incident Reporting

It is the responsibility of every Department of Health employee and volunteer to report any suspected breach of confidentiality or security as well as any violation of policy or procedure to his/her supervisor or designated security coordinator. When a security breach occurs, there are specific Incident Report forms that will be filled out and kept in secured areas as they are strictly confidential.

What good does it do to report a breach once it has already happened? Wouldn't that just be "tattle-tailing"?

Incident reporting is not done to get someone in trouble. The Department of Health does not have any vicious inquisition policy. Rather we are just trying to safeguard information. The reason for incident reporting is so that we minimize the consequences of the breach. Information breaches are different than other security hazards in that once information has gotten into the wrong hands, there is no way to get it back. For example, if a nurse accidentally tells a client's spouse that the client suffers from a newly acquired STD, a breach has occurred. There is no way to reach into that person's mind and get that information back.

When an information security breach occurs, there are only two things that the Department can do: try to stop the information from traveling any further, and take steps to prevent such breaches from reoccurring in the future. Both of these measures attempt to minimize the consequences of the breach. However, none of this can be done without the Department's knowledge of the breach.

If you're hesitant to report incidents because you don't want your co-worker to get in trouble, you must realize that the Department, the client, and your co-worker, will suffer much greater consequences if the breach is left unreported as it may easily grow and grow in severity. Plus, your co-worker will be more likely to commit another breach if the Department, has not had the opportunity to train him or her as to how to better handle the situation. By reporting the suspected breach, you have increased awareness throughout the department.

Things to Look For

Like the defensive driver who watches for unsafe conditions, a risk aware Department employee watches for unsafe conditions such as inadvertent breaches, intentional breaches, and disgruntled employees.

Inadvertent Breaches

Most of the breaches and suspected breaches within the Department of Health are inadvertent on the part of the employee. Conditions such as accidents, carelessness, lack of planning, and lack of knowledge, all contribute to inadvertent breaches. Therefore, to be risk aware, you must help your fellow co-workers to safeguard information by helping them to see the risk of the situation and reminding them of how to reduce that risk.

Some of the more likely locations where one might inadvertently release information would include:

- Elevators
- Social situations
- Hallways
- Smoking or breaks outside the building
- Lunch - outside the building or in a public restaurant

Intentional Breaches

Intentional breaches are breaches in which the employee who causes the breach knew that what they were doing was considered a breach and continued to do it anyway. There can be many reasons for this (one being a disgruntled employee which we will talk about next), most however are not for vindictive purposes. Some employees become negligent by slowly growing complacent with their compliance to departmental policies and procedures. Such negligence can be the cause of many security breaches. Sometimes the temptation to share information inappropriately causes many to gossip or share stories which are security breaches and can be detrimental to the person(s) being talked about. Whenever your fellow co-workers attempt to gossip with you or somehow inappropriately share information with you, remember it is a security breach if the information does not help you to do your job.

Disgruntled Employees

One of the greatest risk of sabotage to information security, computer systems, and overall client care are disgruntled employees. These people, for whatever reason, will commit security breaches in vengeance to purposely hurt the Department, employees, or clients. These breaches may be as notable as an employee giving confidential information to the press, or as obscure as purposely entering incorrect information in the Department's computer database in order to corrupt information integrity. Whatever the breach, these acts absolutely must be reported. If any employee seems disgruntled and mentions to you of their plans to hurt the Department by committing a breach, report this to your supervisor without waiting for the breach to be committed.

Penalties that can be avoided by being risk aware

When employees flagrantly commit security breaches, they can suffer penalties ranging from disciplinary actions such as suspension or dismissal, up to criminal sanctions such as jail term and/or fines.

Summary

In any of the above situations, remember that we are all part of a team that is together trying to serve the public, and that we must notify our supervisor of any suspected breaches or policy violation. Your job depends on you being aware of the potential security risks around you.

Remember that information security is an inside job.

Section V Review

Competent Clinic's Story

Marge, the front desk receptionist at the Competent Clinic, kept noticing Lisa, the nutritionist keep going in and out of the secured area every fifteen minutes or so. Marge knew that Lisa had authorization to enter the secured area so she wasn't concerned. What she couldn't figure out was why Lisa kept visiting the room so frequently. Finally, Marge couldn't resist and had to ask.

"Lisa, for crying out loud, decide whether your going to stay in the secured area or not," Marge said in a teasing tone.

Lisa laughed. "I know, I'm sorry. It's just that I've been expecting a very important and highly sensitive fax from Hazard Clinic. They said they were going to send it over an hour ago. I haven't seen any signs of it at all. I called back, but the person sending it to me is at lunch and nobody else knows anything else about it."

"Well, I haven't heard anything," replied Marge. "Have you checked the front office fax?"

"No, it wouldn't be there. This is confidential stuff. It should only go to the fax machine in the secured area. I gave them the right number." Lisa stopped to think. "Maybe they lost the number or something." Lisa walked over to the front office fax machine, and picked up some papers and looked through them.

"Hey, this is it. Oh my goodness, it was sitting right here for everyone to see. It says it was faxed an hour ago. This has been sitting here for an hour. And look! They faxed me the entire medical record, when I only needed maybe one page." Lisa was shocked. "I've got to call the Hazard Clinic Administrator about this. This person needs to know how to appropriately fax information before information gets into the wrong hands. Marge, give me Hazard's number."

Describe the level of risk awareness at both clinics.

What should Roger have done to help Lorraine?



Section V Review Questions

Please answer and discuss the following questions with your trainer/supervisor as needed.

1. You are responsible for monitoring your co-workers' behavior with regard to confidentiality matters.

True False

2. The main purpose for reporting suspected breaches of confidentiality is for punishment purposes.

True False

3. You should only report incidents that were committed intentionally.

True False