This is a general awareness training presentation on information security, at the end of which you should …

understand common information security violations that you, as a user, are prone to, … how accountability is established at the UF Health Science Center, … and consequences that follow violations.

Think of information security violations as when you don’t follow information security policies or when you break an information security law.

For purposes of this presentation, we are going to focus on those information security violations that occur at the hands of our information and computer USERS.

These violations can be unintentional and careless or unwitting acts, or they can be intentional acts.

The resulting consequences vary in severity, and

When information security violations are discovered, they subject the user to sanctions.

Most security violations committed by our users are of an UNintentional but careless or unwitting nature.

Let’s point out what you are prone to, so you can avoid committing a violation.
<table>
<thead>
<tr>
<th>Information Security Violations</th>
<th>Users are Prone To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaving confidential documents behind, in public places.</td>
<td>Abandoned confidential document</td>
</tr>
<tr>
<td>Leaving your office or work area unlocked where computers or files holding Restricted information are kept.</td>
<td>Office unlocked</td>
</tr>
<tr>
<td>Leaving your workstation without logging off or activating a locking screen saver. This bad practice leaves information especially unprotected if your work area is in a shared or public area.</td>
<td>Leaving workstation without logging off or activating a locking screen saver</td>
</tr>
<tr>
<td>Failing to adequately secure your portable computers, if you use them. We have seen very serious consequences for this violation.</td>
<td>Failing to reasonably secure a portable computer</td>
</tr>
</tbody>
</table>
Information security violations of an intentional nature generally carry more serious consequences for users. Bypassing or relaxing information security safeguards is a security violation of an intentional nature. Examples include:

- Disabling antivirus updates
- Disabling a password requirement
- Sharing your password
- Sharing your login session

When you bypass safeguards, you open your computer up to hackers who could use it to perform malicious things to ANY computer at the University of Florida.

When you share your password, or logon and allow someone else to use your computer session you are bypassing safeguards. When other people have access to electronic information using your password, their true identity in the system is hidden and their actions appear as yours.

Security violations of an intentional nature also include Abuse of privileges such as:

- Using your access privileges to look up an interesting person’s medical information without a work related reason, or
- Installing illegally acquired software, electronic games or digital music

Information security violations of an intentional and malicious nature are rare, but generally carry the most serious consequences for users. Examples include:

- Intentionally spreading a computer virus on our network and computers, or
- Using your access privileges to acquire personally identifiable information with an intent to commit fraud or other financial gain.

It is not often that these types of information security violations are committed by a member of our workforce, but unfortunately they
have occurred and we now must work to prevent them and respond to them when they happen.

Accountability is used in legislation and our policies to motivate changes in information security practices, and to maintain compliance. You should be aware of how your personal accountability is established and the consequences and sanctions that could apply to you.

Accountability is mandated in laws and policies. Safeguards such as computer activity logging, access monitoring and incident reporting work together to reduce ambiguity and doubt about the cause of a security incident, and whether or not a violation of policy took place. Let's look at how these safeguards help establish accountability.

As a computer user, it is important for you to understand just how powerful computer activity logs are. Today’s technology can easily collect detailed information on computer users, such as what web sites you’ve accessed, or what HSC applications you accessed and when what computer you were using and how long you remained logged on.

In the event of a suspected abuse of your computer privileges, activity logs such as these are accessed to support the investigation. Computer activity logs do not discriminate between work, personal and unauthorized uses of our HSC computers; they are ALL logged and attributed to you.
Computer activity logs can be even more detailed showing the individual records you accessed, and what action you took on them. This is a typical activity log in a healthcare information system.

In the event of a patient complaint of a privacy violation, you can see how a computer activity log can support the investigation, enabling authorities to hold the user Jane Doe accountable for her accesses.

Security cameras are an integral part of safety for the University of Florida. They are now regularly deployed in areas where expensive computer equipment is housed or stored. Video picked up on surveillance cameras has and will continue to be used to support investigations of computer theft and damage.

Federal laws require that we have information security incident reporting policy and procedures in place, which we do. Any workforce member is required to report an information security incident when they suspect one. If you violate a policy or abuse a computer privilege, and it is observed by a co-worker, they are obligated to report it, and are in violation of our policy themselves if they chose to ignore it. This is another information security safeguard that helps to establish accountability.

Accountability is **UN**avoidable when it comes to information security. So what happens if you are accountable for an incident or violate an information security policy?
If you cause a security incident, or make the UF HSC vulnerable to a security incident, you might be required to be retrained or oriented on an information security topic that could help prevent re-occurrence. Your training will be guided by your supervisor, your Unit ISA or ISM.

If you neglect training or policies, more serious consequences might occur and could be far reaching.

Some computer viruses and worms originate from unsuspecting, unaware or uninformed users. At the UF Health Science Center, we share a network with all of the users elsewhere in the University, and with Shands Healthcare. A malicious virus or worm introduced through your computer activity, could be potentially devastating to the productivity of others in your department or elsewhere.

There could be consequences to our Reputation. In August of 2005, an information security breach of UF HSC information on a laptop computer caused us to make a public announcement about the incident. Florida Statutes require public announcement in situations like this, regardless if the individuals affected are patients, students, faculty or staff. Reputation is one of the most important assets of any University. It takes a long time to build and an information security incident can do serious damage to it.
And finally, there could be consequences that apply to you directly, such as:
- Being the center of unwanted attention
- Loss of your computer access
- Disciplinary actions such as a verbal warning or written reprimand
- Suspension of privileges and opportunities normally afforded to faculty and staff in good standing
- More serious incidents can lead to you losing your job and facing legal penalties

These consequences are not pleasant to talk about, but it is important that you know what could happen so you know what is at risk to you personally.

This concludes our general awareness training presentation on accountability and consequences. Remember, consequences can be avoided, but accountability can not. You can avoid consequences by learning about our information security policies, good practices and by following them. Training and awareness are key.

<9.5 minutes>