This is a general awareness training presentation on information security, at the end of which you should understand how sensitive and important the information you use is, so you know how it must be protected.

The UF Health Science Center has four classifications of information:

- **Restricted** information is highly sensitive, legally protected, and very important to keep private to avert a violation of privacy or a legal issue.
- **Critical** information is confidential to the UF HSC or very important to business, academic or research functions.
- **Operational** information is not confidential but it is needed to do work. It would be an inconvenience to your Unit if Operational information were lost or unavailable.
- **Unrestricted** information is not confidential and not used in the operation of your Unit; it is information that could be made generally available to the public.

Examples of Restricted information include:

- Protected Health Information (PHI) which is patient identifiable health information
- Identifiable Student records
- Personally Identifiable Information (PII)
- Social Security Numbers of anyone
- Passwords
- Highly sensitive or individually identifiable research work
- Litigation documents
- Others as defined by your Unit

Restricted does *not* mean the information cannot be used by our institution. It means access must be justified and authorized, and those who are provided with access must take measures to keep the information private and secure.
Recall the phrase *Protected Health Information* or PHI from your HIPAA training. PHI is health information combined with name, or medical record number, or address, or key dates, or family members, or any other information that would personally identify the patient.

Protected Health Information is Restricted.

Recall what student identifiable records are. Individually identifiable student information; name or UF ID or SSN or photo, in combination with grades, demographics, admissions, schedules, class rosters, financial, or any information needed and shared by our faculty and staff about our enrolled or former students. Some exceptions apply such as information you would find about a student in a campus directory like their email address, local or permanent address and phone number.

Student Identifiable Records are Restricted.

Recall that personal identification information (PII) are Names combined with social security numbers, or drivers license numbers or Florida Ids, or any Financial account numbers and access codes, or any other information that could be used to commit fraud using someone else’s identity.

Personal Identification Information is Restricted.

Again, Restricted information can be used, but its use is governed by laws and policies. If you use this type of information in forms, documents, electronic files and databases, and aren’t sure if you are using reasonable security, check with your Unit Information Security Administrator and Information Security Manager to be sure.
Restricted information is important to the Health Science Center.

Critical information is equally as important and may need to be kept private as well.

Examples of information that could be Critical to your Unit are:
- Competitive research work that isn’t identifiable, but that we don’t want released so that we maintain a competitive advantage, or until we are certain of the integrity of the research work.
- Grant application information which becomes important with approaching submission deadlines.
- Grant tracking which may be required by a sponsor, in order to retain a prior awarded grant.
- Certain Courseware that may have been extremely expensive to produce and is necessary to deliver on our teaching mission.
- Financial information
- Personnel information
- And other information that may be classified as Critical by your Unit

Remember, some information may not be private, but could still be Critical because of its importance to be available to carry out the functions of your Unit. Your Unit Information Security Administrator and a Dean, Director or Department Chair determines what information is Critical to your Unit.

The other two types of information are Operational and Unrestricted.

Operational information are things like staff directories, policy and procedures documents

Unrestricted information are things like campus maps and news articles.

These are of lesser importance, but you may find them equally protected by virtue of being stored on the same computer system as Restricted or Critical information.
A table like this should be available to you depicting common types of information used in your Unit and their respective classification as assigned by your Unit Information Security Administrator and Information Security Manager, and approved by a Dean, Director or Department Chair of your Unit. Every Unit uses different information, so tables like this might vary from Unit to Unit.

Do you know the classification of the information you use in your job? If not, you are vulnerable to mishandling it. Contact your Unit ISA or ISM to find out.

You are responsible for keeping information confidential when it needs to be, and using our computing resources in a manner so as not to compromise information and resources on other computers.

Improve your awareness and take the time to become knowledgeable of policies and good security practices known as safeguards. In so doing, you will learn to prevent unintended consequences.

This concludes our general awareness training presentation on information classification. You should be aware of Restricted and Critical information that you use and store in the course of your work, and that it needs to be protected. If you have any doubt about the classification of information you use, contact your Unit Information Security Administrator or Information Security Manager for clarification – don’t assume.

To learn more about your responsibilities and safeguards, continue taking the remaining SPICE general awareness modules and review them regularly.

<6 min>