Information Security **General Awareness Training** **Module 1 –Introduction** **For The UF HSC Workforce**	Information security is new to many people, but has been in practice in some industries for many years. It becomes relevant to us today because of the ease with which highly sensitive information may be accessed, and because of state and federal laws requiring it to be secured.
General Awareness: **Information Security** Prevent Risks Protect Information Threats	This is an introductory general awareness training presentation on information security, at the end of which you should understand: the risks we are trying to prevent what information is required to be protected and how it is threatened
Principles of Information Security	Information security seeks to protect the <u>confidentiality</u>, <u>integrity</u> and <u>availability</u> of information needed by the Health Science Center workforce. Most people think information security is just about confidentiality. You will learn about measures we must take in order to make sure certain information is highly accurate, which is what *integrity* is about. Highly accurate information is important in research? It is likely that information integrity measures are already being applied. There will be other measures we will take to ensure timely and consistent delivery of information through information systems, which is what *availability* is about. The availability principle makes us plan to recover quickly from adverse events like hardware failures and natural disasters.
What Are We Trying to Prevent? • Violating someone's Privacy • Identity theft • Loss of competitive advantage • Loss of computer and network resources • Copyright violations and other illegal uses	Let's take a moment and remind ourselves of the negative events that occur as a result of illegal activities taking place with computers, and permissive security practices. You have heard about situations like these in national news. Perhaps you even know someone who was a victim. Awareness, and good information security practices *on all our part* will help prevent the use of our computing environment for illegal activities like these.

 What Must Be Protected? Information ⓘ Servers and Network Desktop and Portable Computers Offices and Buildings Module 1 - Introduction	Information must be protected, but in order to do that, we have to protect our <u>desktop and portable computers</u>, our <u>servers and networks</u> and our <u>offices and buildings</u>. Information is used and stored in all of these places. Did you know that as a user of a computer connected to our UF HSC network, the things *you do* with *your computer* could cause an outage that impacts many other people who share our network – including healthcare workers at Shands or in our clinics? Awareness and education can help you avoid causing such a problem.
 Protected From What Threats? Computer Hackers Phishing Scams Laptop, PDA Thieves Malware - Virus, Worm, Spyware Weather Computer Accident or Hardware Failure Module 1 - Introduction	There are real external threats that take advantage of an uneducated user or a permissive security practice such as <u>computer hackers</u>, people who write and spread <u>malicious software</u>, *phishing scams* to commit financial fraud, and <u>thieves</u> who steal computers. There are serious <u>weather</u> conditions as you are well aware, that threaten to do damage to buildings and resources within our environment. Computer hardware failures or other damage are common occurrances. Of all of the information used by the UF HSC, how do we identify what is most important to protect from these threats?
 What Is Important? Module 1 - Introduction	Let's start with what *laws* require us to protect. Presumably they get us to focus on the causes of the greatest problems for people.
 What Kind of Information ⓘ ? Individually identifiable health information; health information combined with name, or med record #, or address, or key dates, or family members, or any other information that would personally identify the patient. Protected Health Information (PHI) Module 1 - Introduction	You might recall the phrase *Protected Health Information* or PHI, from your HIPAA training. Health information that individually identifies a patient needs to be protected. But HIPAA isn't the only law that information security practices serve.

	The Federal Educational Rights and Privacy Act, known as FERPA or the Buckley amendment, compels us to protect the privacy of students by controlling access to their records.
	And Florida Statute require us to protect personal identification information of anyone, not just students and patients. This includes our faculty, staff, vendors and clients.
	These laws are intended in part, to protect the privacy of individuals, …..
	and with technology today, information security awareness and practices are an essential part of privacy.

 Other ☑ Important to UF HSC Needs To Be Safeguarded Too Academic ☑ Research ☑ Business ☑ Module 1 - Introduction 13	And it's not just information covered by laws that we have to protect. We have to look beyond the laws at important information that provides a *competitive advantage* or builds the *reputation* of the UF Health Science Center, its faculty and its researchers. And contractual and financial information needed to keep the Health Science Center running. Information you use and information you store is information in your custody.
 You Are Responsible Know Your Responsibilities Learn About Safeguards Review The SPICE Training Regularly http://security.health.ufl.edu/training	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 knowledgable of good security practices known as safeguards. In so doing, you will prevent unintended consequences.