



School of Medicine  
UCR Health

# SOM Privacy and Security Training

UNIVERSITY OF CALIFORNIA, RIVERSIDE



# **Welcome to the Privacy and Security Training**

**This course is designed to provide UCR School of Medicine and UCR Health employees with information about their responsibilities in preserving and protecting patient, employee, research and business information.**

# Overview of Training

This training consists of three (3) related training modules, as described below. The estimated time to complete each module is shown so that you can allocate your time accordingly.

Title of Module	Estimated Time to Complete
Privacy and Protected Health Information (PHI)	15 - 20 minutes (approx.)
Risks of Data Breach	10 - 15 minutes (approx.)
Information Security and Awareness & Final Exam	25 - 30 minutes (approx.)

# Overview of Training

Because there are three separate modules within the **Privacy and Security** training, it may be beneficial to take a break at certain points in the training. These logical points will be noted within the training. **When you resume the training, you will return to where you left off without the need to bookmark your spot. However, if you start a review question or quiz, you must complete it in its entirety before exiting the training, or lose your work.**



# Who is Impacted by HIPAA?

Privacy and Security Training (or equivalent UC training) is required by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) for all workforce members of UC's designated Single Health Care Component (SHCC). The SHCC is comprised of:

- The medical centers and clinics at Davis, Irvine, Los Angeles, San Diego, San Francisco, and the medical school in Riverside



# Who is Impacted by HIPAA?

- Clinical operations of the health professional schools at various campuses that, as individual organizational units, perform covered functions (i.e., as healthcare providers, engage in covered transactions)
- Student Health Centers at all campuses
- Occupational Health Centers at some campuses
- Internal Employee Assistance programs (i.e., staffed by UC employees and operated using UC resources); and
- Any other UC entities that engage in covered functions with Protected Health Information





# Who is Impacted by HIPAA

This training is also required for all workforce members of UC's designated Single Health Plan Component (SHPC), which is comprised of UC's self-insured health or group health plans.





## **PRIVACY TRAINING MODULE**



# OVERVIEW – Privacy Training

At various points in this training, you will be asked up-front questions, such as *"What do you think?"* or *"What would you do?"* and asked to pick the best option from a list of options. This means that you may be asked questions before you are presented with all of the information.



# OVERVIEW – Privacy Training


If you are not sure of the answer to a question, start by asking yourself:

- What types of personal and health information would I want protected?
- Under what circumstances would I want others to view or use this information?



# OVERVIEW – Privacy Training

The following questions should guide your thinking as you progress through this course:

- What types of information must be protected under state and federal privacy laws?
  - How can I maintain the privacy and security of protected information and why is it important?
  - What rights do patients have regarding access and use of medical information?
- 
- What are my responsibilities for reporting incidents?
  - What are the consequences and financial penalties for non-compliance?

# INTRODUCTION - PRIVACY LAWS

State and federal privacy laws require that we protect an individual's personal and medical information.



At the end of this lesson, you will be able to:

- Identify the types of information required to be protected under California's state privacy laws
- Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA)
- Identify if the information you come in contact with at work needs to be protected

# PERSONAL INFORMATION

California state privacy laws require that we protect an individual's personal and medical information. This includes:

- Protecting personal and financial information
- Protecting medical and health information

Personal information is a person's first name (or first initial) and last name combined with one or more of the following:

- Social security number (SSN)
- Driver's license number
- California identification number
- Credit, debit card, or bank account number (with PIN or password)
- Medical information



# MEDICAL INFORMATION

California state law also protects a patient's medical information.

- According to Confidentiality of Medical Information Act (CMIA), medical information means any individually identifiable information in the possession of or derived from a provider of healthcare service, health plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. (California Civil Code 56.05(g)).
- CMIA prohibits disclosure of "medical information" without prior authorization unless permitted by law (California Civil Code 56.10)





# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT-“HIPAA”

The “Administrative Simplification” section of Health Insurance Portability and Accountability Act (HIPAA) is federal law enacted to:

- Protect the privacy of a patient’s health information
- Provide for the physical and electronic security of Protected Health Information
- Simplify billing and other transactions with Standardized Code Sets and Transactions
- Specify new rights of patients to approve access/use of their medical information

# HIPAA

If the following identifiers are (1) created or received by a healthcare provider, health plan, or health care clearing house, and (2) relate to the past, present, or future physical or mental condition of an individual, payment for healthcare or the provision of healthcare to the individual, then they would qualify as Protected Health Information (PHI) and are protected under HIPAA.



# HIPAA

## Identifiers:

Name	Dates of Treatment
Address	Account #
Phone	Certificate/License #
Fax	Device Identifiers & Serial Numbers
Email Address	Vehicle Identifiers & Serial Numbers
Social Security #	URL
Date of Birth	IP Address
Medical Record #	Biometric Identifiers, including fingerprints
Health Plan ID#	Full face photo and other like image

# HIPAA

We must protect all forms of personal and health information which include:

## ***Written***

(Documents, mail)



## ***Spoken***

(Phones, conversations)



## ***Electronic***

(Computers, mobile devices)



# PERSPECTIVE

There are a lot of different pieces of information that we need to protect in the course of our work. Because of this, it can be difficult to remember all of them.

One tip to remember, instead of trying to remember all of the details, take a step back and look at the bigger picture:

*Ask yourself: “Does the information I am using help identify a person in some way?”*

If it does, you should treat it as protected information. If you are not sure, you should **STOP** and ask your supervisor. Your supervisor can provide direction and support.



# SUMMARY

You have completed the lesson for **Privacy Laws**.

You should now be able to:

- Identify the types of information required to be protected under California's state privacy laws
- Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA)
- Determine if the information you come in contact with at work needs to be protected





## **PROTECTED HEALTH INFORMATION (PHI)**

**It is important to protect every patient's Protected Health Information (PHI). This training module provides you with an understanding how to provide this protection.**

# Protected Health Information (PHI)

It is important to protect every patient's Protected Health Information (PHI).

At the end of this module, you will be able to:

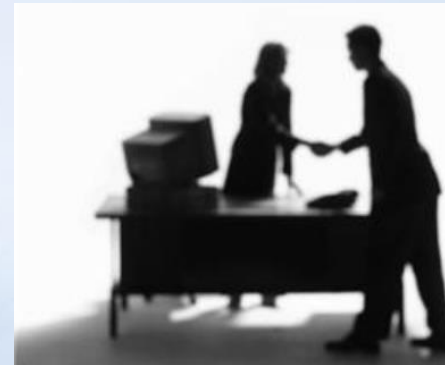
- Identify examples of patient privacy rights that patients have to help protect their own health information
- Identify specific examples of what you can do to protect patient information
- Identify guidelines for when you can/cannot access, use, or disclose a patient's Protected Health Information
- Identify guidelines for when it is okay to use/disclose PHI for Patient Treatment, Payment Services, and Health Care Operations

# HIPAA Gives the Patient Specific Privacy Rights

The following provides examples of some of the specific privacy rights that patients have. These rights are explained in greater detail in the **Notice of Privacy Practices** that patients receive. (See the **Resources** tab in the upper right-hand corner for copy of Notice of Privacy Practices.) We will review the **Notice of Privacy Practices** shortly.

- Patients can request access to and/or copies of their medical record.
- Patients can request amendments to their medical record.
- Patients can request restriction of Protected Health Information uses and disclosures.

NOTE: You should consult the Compliance and Privacy Officer before granting such requests.



# HIPAA Gives the Patient Specific Privacy Rights

Patients can request confidential forms of communication:

- Mail to P.O. Box instead of address
- No message on answering machines



We must accommodate all reasonable requests.

Patients can request an accounting or a report of who obtained their information without their authorization.

# Notice of Privacy Practices

One way that we protect patient information is by giving each patient a **Notice of Privacy Practices** before we use or disclose their Protected Health Information.

In order for the University and its workforce members to use or disclose Protected Health Information, UC must first give each patient a **Notice of Privacy Practices**.

This notice:

- Describes how the University may use and disclose the Protected Health Information
- Advises the patient of his or her privacy rights



Please see **How We May Use and Disclose Medical Information About You** as part of the **Notice of Privacy Practices**.

# Patient Signature is Required

- Healthcare providers must attempt to obtain a patient's signature acknowledging they received the **Notice of Privacy Practices**.
- If a signature is not obtained, the University must document the reason why.
- Health Plans must mail the notice to enrollees.
- The **Notice of Privacy Practices** may not be modified by the patient or patient's representative.





# How Do We Protect Patient Information?

Another way that we protect Protected Health Information is by only using or disclosing patient information if it's required for our jobs, and by only using the minimum amount of Protected Health Information that we need to do our jobs.

There are three things you can do to protect patient information:

1. Only use Protected Health Information if it's necessary to perform your job duties. If you don't "need to know" the information to do your job, you shouldn't access, view, or use the information.
2. Only use the minimum information necessary to perform your job. If you're not sure, ask your supervisor for guidance.
3. Follow UCR School of Medicine policies and procedures for information confidentiality.

# Accessing Protected Health Information

The minimum necessary standard and the “need to know” principle apply to all uses and disclosures of Protected Health Information for payment and healthcare operations.

If you are unsure whether access to Protected Health Information is permitted, ask yourself the following:

- *Do I need to access the Protected Health Information to do my job here at UCR School of Medicine?*

Note: Access for research requires specific Internal Review Board (IRB) approval.

- *Should an employee look at or share another employee’s medical/personal information, if the information is not required for his/her job? (No!)*



# Accessing Protected Health Information

- *How would I feel if someone viewed or discussed my Protected Health Information without authorization?*
- *Do not look at your information or your family's information.*



# Using Protected Health Information

Here are some guidelines for when you can use or disclose Protected Health Information:

## Patient Treatment

You may use and disclose medical information about a patient to those involved in the patient's care, such as doctors, nurses, technicians, providers.

## Payment Services

You may use and disclose medical information about the patient, in order to bill and collect payment for the services the patient received.

[See Notice of Privacy Practices.](#)

# Using Protected Health Information

## Operations

You may use and disclose medical information for healthcare operation purposes, such as: teaching, medical staff peer review, legal purposes, internal auditing, to conduct customer service surveys, and general business management.

[See Notice of Privacy Practices.](#)

# When We Need to Get Written Authorization

We mentioned before that we must attempt to obtain a patient's signature to acknowledge they received the **Notice of Privacy Practices** before being able to use or disclose Protected Health Information (except in emergency situations).

As we continue, we will look at other circumstances where we are required to obtain a patient's prior written authorization before being able to access, use, or disclose Protected Health Information.



# When We Need to Get Written Authorization

There are a number of other situations when we need to get a patient’s (or legal representative’s) prior written authorization before being able to access, use, or disclose Protected Health Information. In these situations, use the official UC HIPAA form (see **Resources** tab). For example, we need prior written authorization before:

- Disclosing medical information or providing records to someone other than the patient, such as:

Employer	Family Member	Friend
Lawyer	Life Insurance Agency	Others

- Disclosing information for use in research (clinical trials)
- Disclosing patient’s information for marketing, fundraising, or mass communication (TV, radio, news) unless an exception applies

# Communication With Patient's Family and Friends

Unless the patient has prohibited a disclosure, care providers must use professional judgment when determining when to share patient information with family and friends.

It is appropriate to share information about a patient with family and friends when:

- The patient explicitly or implicitly consents to the sharing.
- If patient is unable to communicate, use professional judgment.
- Minimum necessary standard applies:  
(1) Don't reveal past medical problems, unrelated to the patient's current condition, and (2) the information should be limited to updates about patient's condition and treatment.



# Disclosure by Phone

- Facility Census/directory: Unless patient has opted-out and does not want to be listed in the directory/census, we can only disclose the location and general health status if the caller identifies the patient by name.



- If the caller requests additional information on the patient, under HIPAA you can provide information to friends and family involved in the care of the patient. Difficulty is often in identifying which friends and family are those involved in the patient's care.

# Disclosure by Phone

## General Guidelines

- Provide information about general condition (unless opted-out of directory) only and refer caller to designated family representative for details.
  - ✓ If the patient is alert and awake, ask the patient if they want to talk with the caller.
- If the patient is able and consents to take the call, transfer caller to patient.
- Otherwise, no information can be provided unless the patient has previously provided a written authorization to disclose the information to the caller.

# Phone Calls – Outpatient Areas

If a friend or family member is calling to verify an appointment or obtain information about a specific patient, before sharing any PHI:

- Check any restrictions on disclosures.
- Ask to speak with the patient if available to confirm their consent.
- Use your best judgment if you know that the caller has been involved with patient care/clinic visits – implied consent by patient.
- Emergency situation: use your best judgment.

If patient has signed an authorization, verify with caller patient information that they would be expected to know (e.g., full date of birth, full name, mother's maiden name, last 4 digits of social security number, etc.).

Always provide only the minimum necessary amount of information (e.g., only say that patient is ready to be picked up from appointment).

# Examples of Using/Disclosing PHI

There are other circumstances, generally those required by law, where you are permitted to disclose Protected Health Information without the patient's permission. In all such cases, UC policy requires that you consult with a relevant expert, such as a health lawyer, a privacy officer, medical records personnel, etc.

For example, you are permitted to use or disclose Protected Health Information in these situations:

- Certain legal proceedings, such as lawsuits
- To avoid serious threat to health and safety
- For mandatory public health reporting
- Law enforcement for certain activities
- Workers' compensation programs



# Examples of Using/Disclosing PHI

- Cadaveric (dead body) organ and tissue procurement/transplantation
- Research, subject to IRB approval (see UCR IRB [website](#))
- Government oversight activities (see Dept. of Health & Human Services [Guidelines](#))
- UC Riverside, School of Medicine Policies and Procedures, Law Enforcement Policy COM 25.0

**IMPORTANT NOTE:** All such disclosures must be recorded so that we can provide the patient with an “Accounting of Disclosures” if they should request it, which is their right under HIPAA.



# Social Media and HIPAA

The purpose of this section is to provide UCR Health employees with requirements for participation in social media, including UC Riverside-hosted social media, and in non-UCR Health social media in which the employee's UC Riverside affiliation is known, identified or presumed.

- **Privacy:** Never post protected health information (PHI) – no exceptions!
- **Transparency:** Be careful about disclosing patient information as a UCR Health worker. Before posting anything, take a moment to consider HIPAA implications.

# Social Media and HIPAA

- **Responsiveness:** Monitor your webpage and respond to questions and concerns. When appropriate, respond offline.
- **Reporting:** Contact the Compliance and Privacy Office should you have concerns about what you have viewed on a social network.
- **Respect:** You are a member of the UCR SOM community. Be mindful of the information you place on a social media site.

# Social Media and HIPAA

Social media, such as Facebook, pose new risks to patient privacy.

- Staff working in healthcare often want to relieve stress of job by sharing information with others.
- Risk is that although patients are not identified by name, enough circumstantial information can be provided that others will be able to identify the patient.
- NO information about patients should ever be posted to social media sites!

# Social Media and HIPAA

## How to keep this from being you

- A physician in Rhode Island was disciplined for discussing a patient on Facebook.
- The physician was fired from the hospital after posting information about a trauma patient.

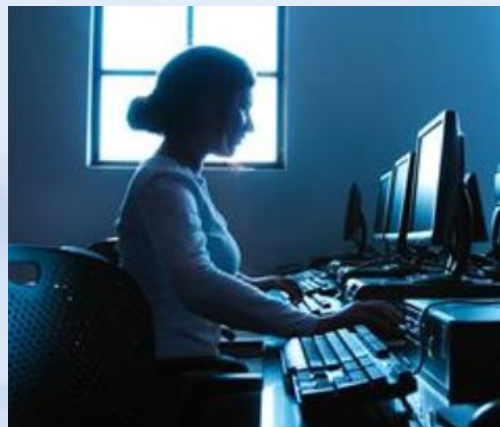


- ✓ The State Board of Medicine also found the physician guilty of unprofessional conduct.
- ✓ The physician did not mention patient name, but included enough information to allow an unauthorized third-party to identify the patient.

# Social Media and HIPAA

## Remember:

- Keep patient information private.
- Other people can see what happens on social media.
- Our professional obligations follow us home.
- Social media includes “Instagram” where pictures are shared with others. Pictures of your EMR or your patients are strictly prohibited!





## **REVIEW OF INFORMATION**



# Review of Information

We will review the information that you have read in this module.

At the end of this review, you will be able to:

- Identify the types of information required to be protected under California's state and federal privacy laws.
- Identify your role in maintaining privacy and security of protected information.
- Identify the risks of privacy and security violations.
- Identify the importance of protecting an individual's personal information.

# Review of Information

- The types of information that must be protected under state and federal laws are personal, financial, health, and medical information.

Name	Dates of Treatment
Address	Account #
Phone	Certificate/License #
Fax	Device Identifiers & Serial Numbers
Email Address	Vehicle Identifiers & Serial Numbers
Social Security #	URL
Date of Birth	IP Address
Medical Record #	Biometric Identifiers, including fingerprints
Health Plan ID#	Full face photo and other like image

# Review of Information

## Role in Maintaining Privacy and Security

Your role in maintaining privacy and security or protected information is:

- Use Protected Health Information only if necessary to perform job duties.
- Use the minimum necessary to perform your job.
- Follow UC Health Sciences or UC campus policies and procedures for information confidentiality and security.

# Review of Information

## Patient Privacy Rights

Patient privacy rights regarding access and use of medical information:

- Patients can request restriction of Protected Health Information uses and disclosures
- Patients can request confidential forms of communication
- Patients can request access to and/or copies of their medical record
- Patients can request amendments to their medical record

# Review of Information

## Importance of Protecting Patient Information

Why it is important that we protect patient information?

- California and federal laws require us to protect certain personal information!
- Privacy violations can harm people!
- It is the right thing to do!
- Failure to protect information can lead to fines and prosecution for UC and you!

# Review of Information

## Resources

### Information Security:

- Your supervisor/manager
- OIT Help Desk: 951-827-7676

### Privacy and Confidentiality

- Your supervisor/manager
- Email: [compliance@medsch.ucr.edu](mailto:compliance@medsch.ucr.edu)
- UCOP HIPAA [website](#)
- Confidential Compliance Message Line: 1.800.403.4744



# Summary

You have completed the **Protecting Patient Information** training.

You should now be able to:

- Identify examples of patient privacy rights that patients have to help protect their own health information
- Identify specific examples of what you can do to protect patient information
- Identify guidelines for when you can/cannot access, use, or disclose a patient's Protected Health Information
- Identify guidelines for when it is okay to use/disclose PHI for Patient Treatment, Payment Services, and Health Care Operations

# Conclusion

The Privacy training component of this course is designed to provide employees with information about their responsibilities in preserving and protecting patient, employee, research and business information. You have completed the **Privacy** module of this training.

Before beginning the next module, **Risks of Data Breach**, this might be a good time to take a break from the training. When you resume the training, you will return to where you left off.





## **RISKS OF A DATA BREACH**

# Introduction

While the Office of Information Technology (OIT) is responsible for some aspects of information security, you have a vitally important role to play in protecting our patients' information.

The risks of a breach of patient information include the following:

- **Electronic Databases**
- **Portable Devices**
- **Email**
- **Faxes**
- **Hardcopies**
- **Human Error**



# Introduction

At the end of this module, you will be able to:

- **Identify the risks of a data breach**

# Associated Risks – Electronic Databases

The greatest risk of a data breach currently (in 2014) is with databases or computer systems of patient information that are on a network that is connected to the Internet. Access to patient information is monitored on a daily basis for unusual or unauthorized access. All staff are accountable for any access to patient information accessed using their unique ID.



**REMINDER:** If you are creating such a database, or using such a system, please ensure that OIT knows about the sensitive information it contains, so that the staff can ensure it is appropriately protected.



# Protecting Patient Information

To protect patient information when using electronic databases:

1. Only access records for patients who you are caring for or have a need for to do your job. Accessing your own or a family member's record is against policy. Requests for family member's information or your own must be processed by the physician's office.
2. Always log out or lock your computer if you are walking away for even a few seconds.
3. Never store patient information on any local machine that is not encrypted.

# Associated Risks – Portable Devices

The second greatest risk of breach comes from databases or files of patient information that are on a portable device.\*

Examples of such devices include, but are not limited to:

- Laptops
- Desktops
- Mobile phones (“smartphones”)
- USB memory sticks
- CDs
- DVDs
- iPads
- Portable Hard Drives



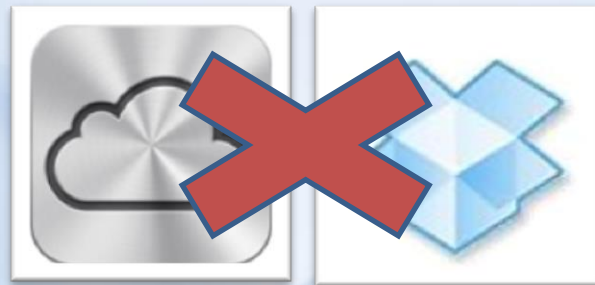
**\*Recall that you can only store protected data on encrypted managed desktops!**

# Associated Risks – Portable Devices

## Storage Services

Personal storage services (e.g., iCloud or Dropbox, etc.) are not permitted. Storage in mobile devices, flash drives, etc. is not permitted, as well. This strict prohibition is due to the high risk of breaches of data being stored outside the University with a service that has no obligation to protect the PHI.

Store all PHI data in secure environments provided by the OIT.



# Associated Risks – Portable Devices

## Mobile Device Security

Mobile smartphones have become a common tool in our industry for email communications. If an email message received on your smartphone includes protected health or other confidential information, this can pose a risk of unauthorized access if the device is lost or stolen since messages can be easily retrieved from the device.

The following are some fundamental smartphone practices that will help protect confidential information on the device from unauthorized access.



# Associated Risks – Portable Devices

## Mobile Device Security

- If you have a work-provided phone and it is lost or stolen, immediately contact the UCR SOM OIT via 827-7676 and request a remote wipe of the phone. Wait to discontinue the service for the phone until after the remote wipe is accomplished. If you discontinue the service on the phone, remote wipe will no longer be available.
- You must enable PIN/password protection on your phone. The more complex the PIN/password, the better. UCR SOM OIT staff can help with this; contact them at 827-7676.

# Associated Risks – Portable Devices

## Mobile Device Security

- Enable the device encryption setting, if available. UCR SOM OIT staff can help with this; contact them at 827-7676. Do not store restricted information on the phone's memory card (SD card) or any external storage that has NOT been encrypted.
- Turn off Bluetooth, Wi-Fi, NEC, and GPS when not specifically in use.
- Do not use mobile devices and mobile phones to take photos of patients – **EVER!**



# Associated Risks - Email

Another source of great risk of data breaches is within email. A great deal of personal information is communicated within email, as much of it is routinely kept within email accounts. It is important to remember that including patient information in your email communication presents a security risk. If an unauthorized person gains access to the email accounts, this personal information is potentially vulnerable.

To protect patient information in email accounts, you may request a secure and encrypted email account, an **@medsch.ucr.edu**, by contacting UCR SOM OIT. Your email will then be secure and encrypted.

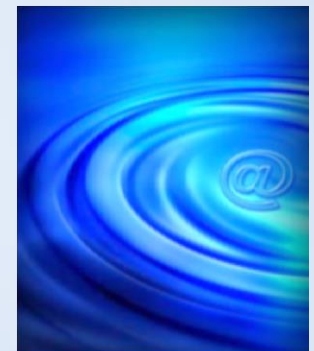


# Associated Risks - Email

## To send secure email:

After having your @medsch.ucr.edu email setup, you will be able to send a secure message from Outlook as follows:

- Put the word **Secure** anywhere in the subject line of the message and then continue typing your subject line. (Example subject line: *Secure: Regarding Your Appointment*).
- Compose your message and send it as you would normally.
- Also, email sent from an @medsch.ucr.edu to another @medsch.ucr.edu is automatically protected.



# Protecting Patient Information

- Protect the email account by using a strong [password](#).

## Password Techniques

- Verify the email address to whom you are sending the email.
- If the email is to be sent outside of the UCR SOM email exchange, it must be encrypted.
- Communicate only the minimum confidential information necessary.
- Emails being sent over the Internet from public locations away from the University should not include restricted information, since these emails are not encrypted.
- Never click on a link within an email or open an email attachment from an unknown source.

# Associated Risks - Faxes

The most commonly reported violation of patient privacy occurs when patient information is either faxed to the wrong fax number, or the fax includes information on another patient, by mistake.

## Protecting Patient Information

To protect patient information when sending faxes:

- Verify the fax number before pushing the send button.
- Double check that only the information on the correct patient is included in the information being faxed.



# Associated Risks - Hardcopies

## Hardcopies

Another risk to patient privacy occurs when patient information is left unattended in areas where anyone can access the area.

Note: Even areas that are designated as “Staff Only” areas can cause problems if the door to the area is unlocked or unmonitored, and anyone can wander into the area.



## Hardcopies - Protecting Patient Information

To protect patient information left in unattended areas:

- Keep papers with patient information on it covered and placed in an appropriate secure area, folder, or cabinet.

# Associated Risks - Hardcopies

- Ensure that when you leave the area unattended, no patient information is left out.
- Dispose of material containing patient health information in a confidential shred container.
- Ensure that patient information on whiteboards or computer screens is not visible to anyone walking by.
- Do not prop doors open, making the confidential information accessible to anyone walking by.
- If you see someone in an area where patient information is being used, verify that they have a job responsibility to be there by confirming that they have an ID badge. If the person is a vendor, they should be accompanied by an employee.

# Associated Risks – Human Error

## Discharge of Patients

Another common problem can occur when a patient is being discharged. It has been reported that sometimes information from another patient's file is mixed into the file of the patient being discharged. This can be particularly harmful for the patient if the information includes their diagnosis, treatments, and medications.





# Associated Risks – Human Error

To protect patient information when discharging patients:

- Double check that you have the correct patient and the correct information.
- Ensure that you've correctly registered the patient under the correct Medical Record Number.
- Ensure that you've correctly entered the information into the correct record.
- Confirm that you have printed out the correct record.





# Associated Risks – Human Error

## Protecting Patient Information

### ***1. Faxes going to the wrong location or include information on another patient.***

**TIPS to prevent:**

Double check the fax number before sending.



Verify that the information belongs to only that patient.

Use two patient identifiers when disclosing information (i.e., not patient in Bed 25, but name and MRN).

### ***2. Giving patient information on another patient.***

**TIPS to prevent:**



Double check the information before handing to the patient.

Triple check if you are printing to a printer that others use, as well.

Double check the printer name and location before printing.



# Associated Risks – Human Error

## ***3. Disclosing information on patients to family or friends visiting the patients.***

### TIPS to prevent:

Always ask a visitor to leave the room if you are going to discuss health information with the patient.

Let the patient know that you need to talk to them about their health information if they say the visitor can stay.

Be careful when disclosing patient status to a visitor, even a casual question about why they have to gown before going into see a patient can reveal information the patient does not want shared with all of their family and friends.

Don't discuss patient information with family members unless you are absolutely positive that the patient has authorized disclosure of information to that family member.



# Associated Risks – Human Error

## ***4. Sending PHI in email distribution lists to staff who do not need the information.***

### TIPS to prevent:

Make sure your email distribution list is up-to-date.

Only include individuals who need the information to care for the patient or for their job.

Limit the information to the minimum necessary.

If the patient's individual information is not needed, don't include it!

The sender of any email containing PHI is responsible for ensuring that the recipient's address is within the [medsch.ucr.edu](mailto:medsch.ucr.edu) email system.



# Some Recent Headlines



- Cignet Health in Maryland assessed fine of \$4.3 million by DHHS for failing to provide records to patients on request.

Patients have the right to obtain copies of their medical record – California requires records to be given to a patient within 15 days.

- UCLA received a \$16 million class action lawsuit for a stolen encrypted laptop. Also missing was the password for the encryption (16,000 patients with \$1000 fine per patient) from 2011.
- Stanford received a \$20 million class action lawsuit for information posted on the website (patient name, MRN, admission and discharge dates, diagnosis codes and billed charges) by a Business Associate in error.

# Some Recent Headlines

- Sutter Health lost an unencrypted desktop PC with patient info on 4 million people, including addresses, dates of birth, phone numbers and email addresses. Even if encrypted, do not leave a password with the device.
- In December 2013, healthcare giant Kaiser Permanente notified approximately 49,000 of its patients of a privacy breach at one of its centers in California. A computer flash drive containing patient names, dates of birth, medical record numbers, and detailed medication information was discovered missing. Additionally, the data was not encrypted nor password-protected.

As stated earlier, all PHI data must be stored in a secure environment provided by the OIT.

# HIPAA Regulations

HIPAA regulations stipulate that electronic communications that contain Protected Health Information (PHI) must be transmitted in a manner that protects the confidentiality of patient information. When you send, receive, or store any electronic document that contains UC Riverside, UCR School of Medicine, or UCR Health confidential or patient information, you are responsible for ensuring the information is processed securely.





# Summary

You should now be able to:

- **Identify risks of a data breach**



# Conclusion

You have now completed two of the three modules of the **Privacy and Security training**.

Before beginning the last module, **Information Security Awareness**, this might be a good time to take a break from the training. When you resume the training, you will return to where you left off.





## **INFORMATION SECURITY MODULE**

# INTRODUCTION

Most cases of compromised computer information at the University are the result of unintentional actions, or inactions, and could be prevented by following basic good information security practices.

Although most UC faculty and staff would never intentionally do anything to put their own or another person's personal or private information at risk, the unintentional exposure of such information does occur at the University with some frequency.

While no course can provide do's and don'ts for every circumstance, the purpose of this overview is to raise awareness of information security and good information security practices in order to help prevent unintentional compromises of sensitive information and computing systems.

# INTRODUCTION

At the end of this course, you will be able to:

- Have a basic understanding of information security and general practices that support information security
- Understand your role in protecting information and privacy - the University's, other people's, and your own



# PURPOSE AND SCOPE

Information security training is designed to raise awareness of good information security practices in order to prevent unintentional compromises of sensitive information and computing systems.

Adopting behaviors that protect information not only benefits the University, it can benefit you and your family, as well.

It is important to keep in mind that no course can address every circumstance for every individual.

It is always a good practice to work with your technical support staff and your information security staff on any question about how best to protect the information you are handling.

# PURPOSE AND SCOPE

The goal of Information Security is to protect data and information against unauthorized access, dissemination, modification, and destruction.

Information security also helps to maintain the privacy of individuals from whom personal details have been recorded. This is important for both ethical and legal reasons.

Information security employs technology and people to reduce the risks to the confidentiality, integrity, and availability of information.

Everyone has a responsibility to protect University information assets. Whether or not you work directly with sensitive information, your work is connected in one way or another with those who do.



# CLASSIFICATION

You have a responsibility to know the sensitivity of the information you are working with and to engage in good practices which protect all University information. See also Family Educational Rights and Privacy Act (“[FERPA](#)”).

The University classifies information in these three general categories:

## **Confidential:**

Information with some degree of sensitivity requiring some degree of protection or restricted access. Unauthorized access to or disclosure of information in this category could seriously or adversely affect the University and cause financial loss, damage to the University’s reputation, loss of confidence or public standing, or adversely affect a University member or partner.



# CLASSIFICATION

## Restricted:

Any confidential or personal information (information that personally identifies or describes an individual) that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

## Non-Confidential

Information which does not fall in the “Restricted” or “Confidential” categories. No special protective measures are required. Proper management of the information will usually ensure its integrity.

# CLASSIFICATION

## Classification Examples

### Confidential

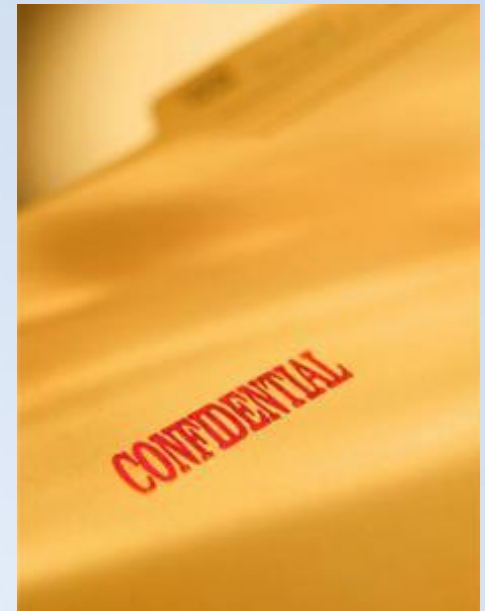
- Intellectual property
- Many types of student records
- Third-party proprietary information
- Home addresses and home telephone numbers

### Restricted

- Social Security numbers
- Medical conditions
- Passwords
- Credit card information

### Non-Confidential

- Service catalogs, course catalogs
- General Information about the University
- Public information about employees (e.g., salaries, department of employment)
- Campus maps



# RISKS, THREATS, AND CONSEQUENCES

Unauthorized access, distribution or publication of sensitive information could have a financial or legal impact on the University and/or you.

## ***A Special Note about Personal Information:***

Various state and federal laws have been enacted to protect the personal information that an organization is entitled to collect and maintain. Most such laws share a common feature: the information obtained must be essential to providing the service requested by the individual.



# RISKS, THREATS, AND CONSEQUENCES

In other words, if the organization can provide its services without obtaining a particular kind of personal information, it should not collect it.

Any time an organization fails to comply with these different laws, it risks fines and possible criminal proceedings. UC may also be required to notify affected individuals if certain types of personal information are inappropriately accessed or disclosed.



# BEST PRACTICES

Every kind of information should be protected based on its classification level. Here are some best practices to consider when handling information:

1. Know what data you have and handle it in a manner consistent with its classification.
2. Make sure you have permission to access the information you are handling.
3. Only collect and handle other people's personal information for legitimate purposes in accordance with UC's mission. Transmit and store it securely. Don't share other people's personal information outside of legitimate business purposes.
4. Don't disseminate restricted or confidential information unnecessarily or post it to social media websites.

# BEST PRACTICES

5. Don't transmit restricted or confidential information by email, which generally does not afford adequate security.
6. Don't leave restricted documents in view of wandering eyes or in public place.
7. Store protected information in secure file storage locations provided by OIT (EMRs, HIPAA-compliant storage, etc.).





# Conclusion

## Information Security:

- Measures serve to protect information against unauthorized attempts to access, use, modify or destroy information assets.
- Must be applied to all data, information, and information assets in any form. This means information in electronic and non-electronic form.
- Provides a framework to ensure the security of technological infrastructure, services and components involved in the processing of information.
- Information security ensures the confidentiality, integrity and availability of information.
- Information security protects the privacy of other people's information.



# Conclusion

Knowledge of the sensitivity of the information one handles is essential to the appropriate safeguarding of that information.



Everyone has an important role to play in protecting and preserving the confidentiality, integrity and availability of University information, as well as the privacy of other people's information.

Information security reduces the risk of threats to information assets and is everyone's responsibility.



## **SOCIAL ENGINEERING**

# Social Engineering

Social engineering is the process of obtaining information by manipulating and exploiting the goodwill of others.

- The social engineer typically calls or sends an email pretending to be someone else or shows up at your workplace under false pretext.
- Social engineers are interested in gaining access to organizational and personal information, primarily to perpetuate a fraud, commit industrial espionage or simply to disrupt activities.
- A “social engineer” is on the lookout for bits of information that can help him or her assume someone else’s identity, usually without that person’s knowledge.

# Social Engineering

The information they want includes:

- Passwords
- Personal information
- Bank account and credit card information
- Sensitive business information

Social engineers exploit the trust, courtesy, naiveté, lack of knowledge, and goodwill of others.



# Social Engineering Tactics

Social engineers use a variety of methods to steal or trick you out of the information they want.



Some social engineers use email to try to pass themselves off as an individual or business (such as a financial institution) that you are likely to trust. They email requests to their prospective victims for information on their financial or computer accounts and credit cards.

Legitimate organizations do not email their customers asking personal or confidential questions, or asking for passwords. When in doubt, do not respond and contact the organization directly.

# Social Engineering Techniques

Below are some of the methods social engineers use to try to steal or trick you out of the information they want:

- ***Malicious software:*** They exploit human curiosity in delivering malware. Such code usually arrives in the form of an attachment or link offering something of interest, such as an e-card or video. When you open the file or click on the link, you activate the virus.

**Never click on any suspicious link via email. If in doubt, please send your email to the helpdesk ([helpdesk@medsch.ucr.edu](mailto:helpdesk@medsch.ucr.edu)).**





# Social Engineering Techniques

- **Phishing:** They attempt to trick you into revealing confidential, personal or financial information, your password, or into sending money. Any such attempt is in person, over the phone, via email, instant message, text, Facebook, Twitter, etc.
  - Smishing: Phishing via text (sms) message
  - Spear Phishing: Highly targeted phishing
  - Vishing: Phishing over the phone (voice)
- **Dumpster diving:** They search for invoices or other documents containing sensitive information in your trash.
- **Eavesdropping:** They obtain sensitive information by listening to private conversations.
- **Impersonation:** They try to pass themselves off as a trusted individual or entity or some other person who would not normally arouse suspicion by requesting information.



# Risks, Threats, and Consequences

Social engineering is a method of obtaining information through trickery. The social engineer tries to exploit your trust.

A “harmless” gesture, like tossing a document in a wastebasket or giving your password to someone who says he or she is an “IT person”, can give the social engineer an opportunity to commit harm. The consequences may not only affect the directly targeted victim, but the organization itself.



# Risks, Threats, and Consequences

Consequences of social engineering include:

- Identity theft
- Theft of restricted or confidential data and information
- Unauthorized use/abuse of computers
- Legal proceedings against an individual or an organization that is the victim of a social engineer
- Loss of confidence in the University



# Best Practices

Social engineering attacks can be easily prevented.

The following best practices will help ensure better protection for your personal information and the University's sensitive and confidential information:

- Don't give private information to anyone you don't know or who doesn't have a legitimate need for it (in person, over the phone, via email or the Internet).
- Be cautious about what you say in elevators, restaurants, trains, buses and other public places.
- Your passwords belong to you. Never disclose them to anyone.
- Shred sensitive information. Never put it in the garbage intact.
- If an unknown party is present in your office, request identification and escort the stranger to his or her host.
- Report suspicious behavior and dubious calls to your supervisor.

# Conclusion

- Social engineering is the process of obtaining information by manipulation and trickery.
- Social engineers take advantage of other people's trust, courtesy, naiveté, lack of knowledge, or desire to be helpful as a means of gaining access to personal or confidential information.
- Anyone can be the target of social engineering attacks.
- Protect yourself by keeping your username and password secret and never disclose them to anyone.
- Don't let anyone into your workplace without proper identification.
- Never provide restricted information unless you are sure you know the identity of the person requesting it and the reasons are legitimate. When in doubt, don't provide the information.





# **PASSWORDS**

# Passwords

Passwords are an important control on access to information. Passwords are like a unique key to a lock that only you are allowed to use.

Too many passwords are guessable using easy-to-obtain or automated “password cracking” tool. This can be because of insufficient length or complexity, or the use of first or last names, family members, pets, hobbies, favorite actors, etc.

## ***What can a hacker do with your password?***

- He/she can log in under your name and gain access to any information that you are authorized to access.
- Even if you believe the information to which you have access is unimportant, a hacker can use your password as a springboard to gain access to other systems that you don't even have access to yourself.
- The site the hacker visits and the actions performed are attributed to YOU!



# Best Practices

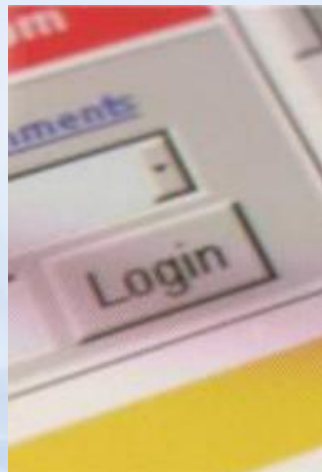
Since a password is often the weak link in the security chain, you can enhance information security by observing the following best practices:

- Always comply with your location's rules for selecting and creating passwords.
- Use a mix of capital and small letters, numbers, and special characters (e.g., \$,!, @, /, &, etc.).
- The longer the password, the harder it is for someone to guess.
- Substitute numbers or symbols for letters: "0" for "O", "@" for "a".
- Don't choose a password with letters that appear on successive keys on keyboard, such as "qwerty". Avoid common keyboard sequences, such as "abcl23".
- Don't choose a password that can be found in a dictionary in any language, whether spelled forward or backward.
- Don't use your username as your password.



# Best Practices

- Don't use personal information: names of family, places, pets, birthdays, address, hobbies, etc.
- Don't write down your passwords or post them in your work area (such as Post-It notes on screen/drawer).
- Never give your password to anyone. Change your password immediately if you suspect someone else may know it.
- Change your password as soon as possible after using a public or untrusted computer.



# Conclusion

- A password is one of the elements used to control access to resources and services.
- Your password is the key to your electronic identity.
- A password's effectiveness is a function of its complexity and your ability to keep it secret.
- Your password should not be easily guessable.
- You should be able to remember your password easily.
- You are responsible for all of the actions performed with your accounts, so your password choice is crucial. Select secure, memorable passwords and keep them secret.



## **MEDIA SECURITY**

# Media Security

The theft and loss of computing devices and documents pose a significant risk to the security of any sensitive information they contain. The risks are even greater for mobile devices.

Physical protection measures play a key role in safeguarding information. Because they are easy to steal, thieves are always on the lookout for:

- Mobile devices (laptops, smartphones, etc.)
- Portable media (external hard drives, etc.)
- Document or reports
- Information transmitted via unsecured wireless networks

# Media Security

Vigilance is the watchword and should be observed both in and outside the workplace particularly in public places, such as lines, airports, restaurants, and conference rooms.

Technological solutions alone will not provide effective security. The human factor is a vital element in protecting information.

Immediately report any loss or theft of computer equipment used for work to your department and technical support person, or the OIT Helpdesk.



# Discretion

Restricted information may in certain instances be accidentally disclosed.

Everyone has occasionally overheard a private conversation that was not for their ears. Usually such situations are insignificant and without consequence. They do, however, pose an important risk of disclosing personal, confidential and restricted information.



Never assume that the person with whom you are talking is the only one listening to what you say. Any discussions not intended for the public should always take place in a private location, away from people who can overhear.

Before beginning the last few sections of this module, this might be a good time to take a break from the training. When you resume the training, you will return to where you left off.







## **WIRELESS NETWORKS**

# Wireless Networks

Wireless technology permits great mobility. At the same time, information sent via standard, unencrypted wireless networks is especially easy to intercept.

To protect personal, confidential or restricted information, only use known, encrypted networks, or encrypt the information itself.

Most coffee shop/hotel/airport-type wireless networks are not encrypted and therefore not secure.

UCRWPA is the UCR's safe wireless network for connecting to networks. Please use VPN to add additional security.



# Risks, Threats, and Consequences

Criminals can gain access to confidential information by:

- Looking at documents left in plain sight on your desk or conference room
- Overhearing conversations
- Stealing unattended computer equipment and mobile devices
- Dumpster-diving in recycling bins and trash containers

Theft not only results in the loss of equipment, but can trigger:

- University notification to individuals whose personal data is lost
- Damage to individuals whose personal data is lost
- Financial loss
- A tarnished reputation
- Legal penalties



# Best Practices

You can help protect information by adopting simple rules or slightly altering your habits and always keeping in mind that mobile devices and portable media are especially vulnerable to loss or theft. The following habits can considerably reduce the risk of an information security breach:

- Use computer security cables to anchor laptop and desktop computers to work surfaces.
- Before leaving your work area unattended, turn off or lock your computer, put away sensitive documents, and lock your cabinets and other storage spaces. Take laptop computers, flash drives, DVDs and other portable devices and media with you, or lock them up.
- Remove sensitive documents immediately from printers, fax machines and copiers so that no one else can read them.
- Shred documents that contain sensitive information. Do not discard them in public wastebaskets.

# Best Practices

- If you encounter an outsider looking for a colleague, escort the person to that individual's office.
- Leave nothing behind when you exit a conference room: wipe the board and pick up all work documents and drafts.
- Protect your computer, laptop and/or mobile device with a complex password. Configure it to lock after a certain period of inactivity.
- Use encrypted desktops to scan restricted information.
- Never store restricted information in laptops or mobile devices.
- Don't leave portable equipment in a vehicle, even if it is locked. In addition to the possibility of theft, the heat in a closed vehicle can sometimes damage components.



# Best Practices

- Avoid sharing a computer that you use for work, including with family members. Sharing computers significantly increases the risk of loss, infection, breach of confidentiality, etc. If you are not the sole user, make sure to create separate user IDs and passwords and always store your work documents in your personal folder.
- Do not keep any confidential and restricted data stored on portable devices. All confidential data will reside on encrypted desktops or Electronic Medical Records.
- Always protect your computer hardware and portable media against theft when traveling. Don't draw unnecessary attention to your baggage or computer equipment and don't leave it unattended.





# Best Practices

- Set your mobile device to ‘ask’ before connecting to unknown networks. Deactivate “Bluetooth” and wireless when you are not using them.
- Always use a secure web connection (“https” in the URL; lock icon in the browser) when you enter passwords to a website or work with sensitive information via the web.
- Always use VPN to connect securely to University resources when working remotely or using wireless network.
- Contact your Technical Support staff (OIT) for assistance.
- Shield personal identification numbers (PINs) and passwords from public view when working on your computer or smartphone in a public place.
- Be aware of what you discuss in places where others may overhear.



# Conclusion

Everyone is responsible for the physical security of information in their possession.

Physical security depends on good habits. Make sure you logout of your desktop and laptop when not in use. Lock your office at the end of the day.

Vigilance is the watchword both at the office and on the road.

At the office or on the road, always be aware of the need to physically secure information.

# Conclusion

Put documents in a locked place and lock your computer before leaving them unattended.

Shred sensitive documents when no longer needed.

Immediately report any loss or theft of computer equipment to Office of Information Technology (OIT).





**EMAIL**

# Email

Email is a powerful communications tool that is a part of the daily routine of millions of Internet users.

In general, the nature of email and the Internet makes it possible for an email to be read by someone other than the intended recipient.

Your @ucr.edu email is not a secure means of exchanging sensitive information. Please request an @medsch.ucr.edu email account for secure/encrypted email capabilities.

In addition to the valuable information email can provide to criminals, it and its attachments serve as an ideal mechanism for infecting your computer system with viruses and other malware. Also remember that the emails you send represent both you and your organization.

# Email-Related Threats

## *Phishing*

The transmission of an unsolicited and seemingly authentic email employing the identity of your organization, a known company or financial institution for fraudulent purposes is known as “phishing.” Recipients are asked to provide confidential or personal information or passwords on some pretext by replying to the email or clicking on a link to a fake web site resembling that of the organization in question.

Note: Any attempt to trick you into revealing confidential, personal or financial information, your password, or sending money is phishing, whether the attempt is in person, over the phone, via email, instant message (IM), text, Facebook, Twitter, etc.



# Email-Related Threats

## *Malware*

Malicious software, or “malware”, such as viruses, Trojan horses, computer worms and spyware, is often transmitted by email through malicious links or attachments. Clicking on these links or opening these attachments will infect your computer. Similar to phishing, these emails often appear to be from your organization, a known company or financial institution.



# Email-Related Threats

## *Spam*

Spam is the transmission of multiple copies of the same email with harmful or unsolicited commercial content to many recipients. Spam is a harmful practice that results in loss of time for users and financial loss for many organizations. Because of the large quantity in which it is distributed, spam can also result in reduced network performance.

Spam serves increasingly in phishing activities and the distribution of malware.



# Risks, Threats, and Consequences

Email lets anyone send messages (texts and attachments) instantly, anywhere in the world. The number, size, and variety of email messages is increasing each day.

Email senders may not be whom they claim to be. It is often difficult, if not impossible, to authenticate an email sender's address. One should never respond to spam or any email from a sender that cannot be authenticated as doing so can lead to more serious problems.

Even if the email sender is who he claims to be, email is not a secure means of exchanging restricted or confidential information.

# Risks, Threats, and Consequences

Improper email use can lead to:

- Identity theft
- Theft or inappropriate exposure of information
- Transmission of malware and infection of multiple systems
- Stolen account credentials/passwords
- Financial loss
- Becoming a victim of fraud
- Flooding of servers and networks and the possibility of crashes or service interruptions
- Tarnished reputation



# Best Practices

Being careful about sending and responding to email messages can help to protect information and your organization, and also reduce spam. Make sure to observe the following practices:

- Don't transmit restricted information by email; the content of email messages is not private during transmission to the recipient.
- Be on guard for phishing. Never respond to email requesting your password or other personal or confidential information.
- Delete spam. Don't reply or forward it. Replying to spammers validates that your address is legitimate and increases the chances they will send you more spam in the future.

# Best Practices

- Don't use a personal email account for work-related activities.
- Keep in mind that it is often difficult, if not impossible, to know for certain who sent an email. Don't click on links or open attachments in unsolicited email unless you can verify their legitimacy.





# Conclusion

Like conventional mail, email is subject to certain rules of use. UC's ethics and acceptable use policies apply to email.

Increasingly, email is used to phish passwords and other personal or confidential information from its recipients, or to trick recipients into clicking on harmful links or attachments, or responding to fraudulent offers.

Spam is a nuisance and offers no value. It is typically sent to large numbers of individuals without their consent and is a serious source of network pollution and malicious content that should be destined for the trash.

# Conclusion

Be on guard for attempts at phishing information.

Email restricted information via Secure Email – using your @medsch.ucr.edu email account.

Resist temptation to open attachments or click on links from an unknown or unverified source.

Don't respond to or forward spam. Just delete it!





# **MALWARE**

# Malware

Malware (malicious software) is an umbrella term for viruses, worms, spyware, Trojan horses, and other destructive computer programs designed to damage a computer system or interfere with or capture its data.

Malware can be used to steal passwords and data, spy on your Internet browsing habits, enable a hacker to seize control of your computer, or even record all of your keystrokes. It can also interfere with computer systems, networks, and an organization's day-to-day operations.



# Malware

Some malware requires human interaction to be installed, such as clicking on a link, opening an attachment, downloading a file, or installing a plug-in.

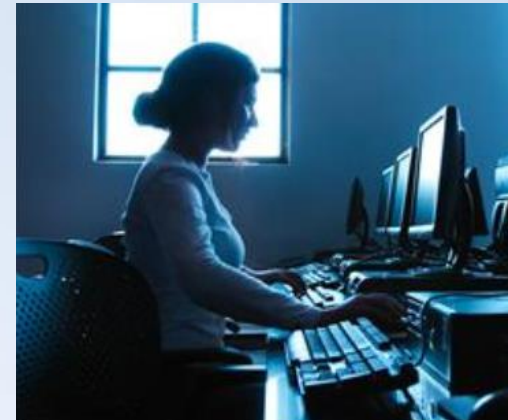
Other malware is designed to propagate with little or no user interaction. In either case, malware can quickly wreak great havoc.



# Sources of Malware

Malware comes from different sources. Most malware is unknowingly installed as a result of:

- Clicking on malicious links in email, texts, instant messages or social networking sites, such as Facebook and Twitter
- Opening email attachments
- Clicking on ads or unknown pop-ups
- Using infected portable media
- (flash drives, CDs, DVDs, etc.)
- Downloading files from the Internet



Malware also can be purposely installed by hackers who exploit a compromised password or other vulnerability.



# Best Practices

Prevent malware infections by observing the following tips:

- Never deactivate your computer's antivirus or protective software. Make sure that protective software and accompanying definition files are updated frequently and automatically.
- Never open an unsolicited attachment. If in doubt, contact the sender and ask if the attachment is legitimate.
- Don't click on unknown links in email, texts, instant messages, social networking sites, ads, or pop-ups.



# Best Practices

Prevent malware infections by observing the following tips:

- Only download files and plug-ins from trusted sources, and don't use untrusted portable media, such as a stranger's flash drive. Also, don't download plug-ins to view pictures, videos, music and other content online without verifying their legitimacy. These often contain malware.
- Contact OIT if you believe your computer is infected with malware. Disconnect the computer from the network immediately to keep the infection from spreading or sending information to an attacker.



# Conclusion

Criminals are often responsible for the creation, distribution and installation of malware.

The term “malware” refers to all types of malicious software, including viruses, worms, Trojan horses and spyware.

Malware poses a potential threat to your information and to the University’s information.

Malware is typically transmitted by email attachments, malicious web pages, web pop-ups, altered programs, portable media, etc.

Many types of malware require action from the user to install. Some of the more sophisticated malware is self-propagating.

# Conclusion

You play an important role in dealing with this threat. Following the practices discussed in this module will help reduce the likelihood of malware infection.

Be prudent when browsing the web, opening email attachments, clicking on links, and downloading or sharing files.

Contact OIT immediately if you believe your computer is infected with malware.





# **CONFIDENTIALITY**

# Confidentiality

The Internet provides access to a multitude of online services. The Internet has also made it more difficult to keep track of and control our personal and confidential information.

Be wary of where you put your personal information, as well as University information.

The information you provide online could end up being used against you or your organization, or in other inappropriate ways.





# Social Networks

The term “social network” refers to web-based applications that are designed to bring together friends, associates, professionals and other individuals who employ or share a variety of tools for staying in touch and swapping information.

Highly effective communication tools, social networks enable hundreds of millions of people around the world to locate and maintain contact with friends, family and co-workers, anywhere on the planet. They also enable evil-doers to find this information.

Information posted to social networks can be easily retrieved, catalogued and recorded. It is also difficult or even impossible to “take back” information you post on these sites.

# Intellectual Property

Many Internet sites acquire ownership of anything you post to their sites. Such sites can subsequently use this information for research or promotional purposes without your consent.

Also be sure to comply with the law when copying material (images and audio or video content) from the web. Unauthorized downloading or sharing of copyrighted materials is illegal.



# Secure Sites

The Internet is now routinely used by millions of people around the world for communication. In addition to being a fantastic source of information, it is used by an ever-increasing number of people to manage their personal finances, make purchases and update information with government agencies, banks and businesses.

You can protect yourself by always transmitting your personal data over a secure link to a reputable site.



The HTTPS protocol provides secure access to banking and other information. Any address starting with https and accompanied by a padlock icon provides a greater level of security for information you send online.

# Risks, Threats, and Consequences

Threats, risks and consequences associated with the Internet:

## *Phishing*

- Identify theft
- Financial fraud
- Loss of confidentiality
- Extortion
- Potential legal proceedings
- Possible impact on your credit rating
- Tarnished reputation



Inappropriate use of social networks can also:

- Tarnish your reputation or that of your organization
- Result in lawsuits for defamation or disclosure of confidential information
- Cause financial loss

Once information is on the web, it is very hard to remove and can be further distributed without your consent or control. What you post to the web may even become the property of the hosting service.

# Best Practices

The Internet offers a goldmine of information and gives users virtually unlimited communications options. Carefully consider the information you plan to disclose when registering for a site or providing information about yourself online. Protect yourself effectively by considering the following:

- Keep your personal information, as well as that of family, friends and co-workers, confidential by not disclosing personal information about yourself or them. An innocent conversation with a “friend” you encounter on a social network could reveal sensitive information that could put you, others, or the University at risk.



# Best Practices

- Don't post personal information about yourself or others - especially information that could be used to:
  - ✓ Know where you live or where you work
  - ✓ Steal your personal identity
  - ✓ Commit fraud or another crime
  - ✓ Identify others without their permission, or identify a minor





# Best Practices

- Beware of strangers
  - ✓ Never accept the invitation of a stranger
  - ✓ If you communicate with a stranger, limit the information which can identify you.
- Use blogs and chat rooms carefully
  - ✓ Be careful of what you write: Never mention your employer or your loved ones
  - ✓ Be careful of the comments you post:
    - Could they be interpreted incorrectly?
    - Do not quote another person without their permission
    - Do not post pictures of another person without their permission
- Use the security and privacy settings of social networking sites to limit access to your personal information.

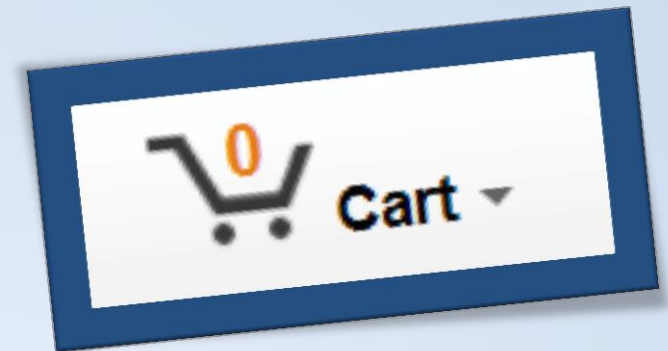


# Best Practices

- When making online purchases or transactions, entering personal or confidential information, or entering your password online:
  - ✓ Use a trusted computer - don't use publicly accessible computers, such as in kiosks or Internet cafes
  - ✓ Make sure your connection is secure by checking for the presence of:

A URL that begins with `https://`

A locked padlock icon in the location bar or a corner of the browser window



# Best Practices

- ✓ The domain name (ex: something.com) does not change after your secure connection has been established.
- Empty your browser's cache memory when you are done.



# Basic Good Computing Practices

Having completed this module, you should now have a basic understanding of information security, general practices that support information security, and your role in protecting information and privacy - the University's, other people's, and your own.

Complementing basic information presented in this course, the following are basic good computing practices everyone should follow - from UC's Minimum Requirements for Network Connectivity (see: Business & Finance Bulletin 15-3: Electronic Information Security, Section IV).

# Basic Good Computing Practices

- Use complex passwords and keep them secret and secure.
- Turn off unnecessary services/programs so others can't use them or take control of your computer with them without your knowledge.
- Set your computer to lock or go to sleep or screensaver when you're not using it, and make sure a password is required to start up or resume activity.

OIT performs the following services:

- Keeps your operating system and applications patched and up-to-date
- Uses anti-virus/anti-malware software and keeps it up-to-date
- Turn on your computer's firewall

# Conclusion

Vigilance is the watchword on the web. Be careful when making purchases, conducting transactions, or socializing over the Internet.

Beware of what you share or post online and remember that you can't "take it back."

Before transmitting any information, check that the site is secure.

Beware of phishing and online scams.



Social engineers can learn much more than you think about you and your organization by patching together information from different sources.



# Conclusion

You should now be able to:

- Protect and preserve the confidentiality, integrity and availability of University information, as well as the privacy of other people's information.





## **IMPORTANCE OF MAINTAINING THE PRIVACY AND SECURITY OF PATIENT INFORMATION**

# Importance of Privacy

It is important for employees to maintain the privacy and security of patient information.

At the end of this review, you will be able to:

- Identify the importance to maintain the privacy and security of patient information
- Recognize how to report violations in privacy and security

# Importance of Privacy

## Protecting Privacy is the Right Thing to Do

One reason that we need to protect patient information is that it is the right thing to do.

Not only has the public entrusted us to protect the information they have given us, but we also have a moral and ethical responsibility to safeguard personal and health information as though it were our own, or that of our loved ones.

For more information, view the [UC Statement of Ethical Values](#) now or click on the **Resources** tab in the upper right-hand corner.

# Importance of Privacy

## Privacy Violations Can Harm People

We are probably all aware that identity theft is occurring more often. We may even know someone whose credit card or bank information was stolen.

However, we may not realize that identity theft can start with something very simple, like telling the wrong person the name of a patient and where they were treated.

Why? A person could use this information to try to dig up more information, until they have collected enough to cause real harm.

# Importance of Privacy

For example, if someone knows a patient's name and where they were treated they could call a billing specialist and try to get them to send the bill to a new address by pretending to be the patient's spouse or relative. If they are convincing, they may get a lot further than you would expect.

## Privacy Violations Can Result In Fines & Penalties

Violations may result in fines and penalties levied against the institution and individuals. Examples of different fines:

Up to \$2500	Disclosing PHI without a "need to know"
Up to \$25,000	Knowingly violate a patient's privacy by obtaining, disclosing, or using PHI
Up to \$250,000	Knowingly violate a patient's privacy by obtaining, disclosing, or using PHI for financial gain



# Importance of Privacy

## Privacy Violations Will Result In Disciplinary Action

In addition to possibly being fined, accessing, using, or disclosing patient information without authorization will result in disciplinary action up to and including termination of your employment, and possible referral to law enforcement, if applicable.

## Reporting a Privacy or Security Violation

To report a privacy or security violation:

- Notify your supervisor or manager right away
- Call the Compliance and Privacy office

# Importance of Privacy

- If it involves electronic information, also contact the security officer
- If there has been a theft of a computer, notify the UCR SOM OIT and/or UC Riverside Police Department

You have completed the review of **Importance of Privacy and Security**.

You should now have knowledge of:

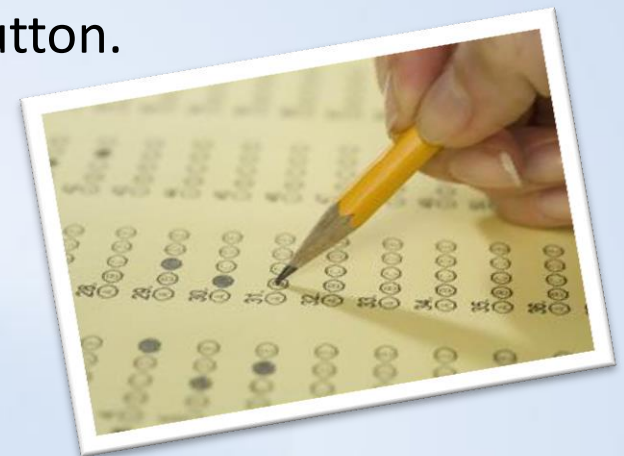
- Identifying the importance to maintain the privacy and security of patient information
- Recognizing how to report violations in privacy and security

# Exam!

The exam will cover content that you have read in the Information Security Awareness module.

As you take the exam, please remember:

- A score of 100% is required to pass the exam.
- Allow at least 5 minutes to complete the exam.
- The questions are multiple-choice and true/false.
- Answer each question by clicking the button next to your selection. Change your selection by clicking another button.
- Click SUBMIT.



# Confidentiality Agreement

By clicking on the **I AGREE** button below, I acknowledge that I have reviewed the foregoing University of California Privacy Training module and Confidentiality Agreement and agree to abide by UC policy and Federal/State privacy laws.

I AGREE

# Conclusion and Exit

## *Congratulations!*

You have now completed the modules on:

**Privacy & Protected Health Information (PHI)**  
**Risks of a Data Breach**  
**Information Security**

To successfully exit this module, please click the EXIT tab in the upper right-hand corner.

