



Menu | Resources | Contacts


**THE OHIO STATE UNIVERSITY**



## Annual HIPAA Privacy & Security

*Please note that this is not interactive and for reading purposes only.  
The test is a separate document.*

© 2016, The Ohio State University

NEXT >

Menu | Resources | Contacts


### Introduction

**Welcome to Annual HIPAA Privacy & Security.** In this course, you will learn how to keep patient information secure.

**After you successfully complete this course, you should be able to:**

- Recognize that privacy and security of sensitive information is your responsibility.
- Identify situations where sensitive information may be handled improperly.
- Identify how you can protect patient and confidential information in common workplace situations.
- Recognize that you will be held responsible for improperly handling sensitive information.
- Determine who to notify if you have questions about the privacy and security of sensitive information.


**Once you complete this course, you will take an assessment. If you pass the assessment with 80% or higher, you have successfully completed this course.**


**THE OHIO STATE UNIVERSITY**

Menu | Resources | Contacts

## Training Overview

**This training and some of the examples are oriented toward Wexner Medical Center (OSUWMC), but the requirements detailed in this training apply to all covered components at The Ohio State University.**




**Audience:** Faculty, staff, and students who access protected health information at OSUWMC and other parts of the University.

**Prerequisites:** None

**Course Length:** You should be able to complete this course in about **30 minutes**.




**Revised:** August 2016


THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

## Ohio State University's Expectations of Employees

*Learn about what The Ohio State University expects everyone to do.*


**i** Remember you may only access information that is needed to perform your job duties! Failure to do so will result in corrective action up to and including termination. Your activity on your EMR may be audited to determine if you have a business need to review a particular patient's medical record.


THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

## Ohio State University's Expectations of Employees


Click each image below to learn about what The Ohio State University expects everyone to do.



**Protect Patient Information.**




**Protect other information such as employee information.**



**Follow the University's and OSUWMC's privacy and security policies as applicable.**

**i** Remember you may only access information that is needed to perform your job duties! Failure to do so will result in corrective action up to and including termination. Your activity on your EMR may be audited to determine if you have a business need to review a particular patient's medical record.

 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

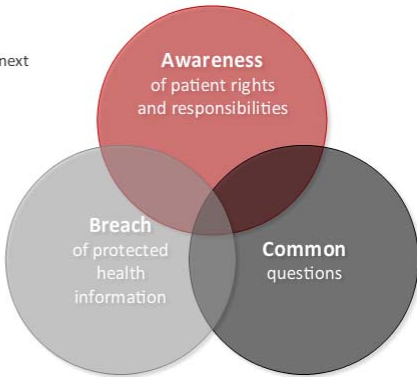
## ABC's of HIPAA Privacy and Security


The Ohio State University is committed to compliance with HIPAA. As faculty, staff, and students who access protected health information at OSUWMC and other parts of the University, you must:

- Take your responsibility to protect a patient's privacy very seriously.
- Acknowledge that violations of the applicable policies and procedures related to privacy and security are subject to discipline up to and including termination.

The ABC's of HIPAA privacy and security are covered in the next three lessons. They include:

- **A**wareness of patient rights and responsibilities.
- **B**reach of protected health information.
- **C**ommon questions.



 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

### Definition of Identity Theft

Identity theft occurs when someone uses another person's identifying information without permission.


The Ohio State University Wexner Medical Center:


- Prevents
- Detects
- Reduces

the harmful effects of identity theft.

**Examples of Identifying Information:**

- Name
- Social Security Number
- Medical Insurance Number
- Credit Card Number
- OSUWMC Badge with Payroll Deduct






THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts


### Identity Theft Red Flags

An Identity Theft Red Flag is a **pattern, practice** or **specific activity** that indicates the possible existence of identity theft.



**Examples of identity theft red flags are:**

- Records showing medical treatment that is inconsistent with a physical examination.
- Identification that appears to be altered or forged.
- Complaints or questions from a patient about information added to a credit report.
- Patient receives a:
  - Bill for another patient.
  - Bill for a product or service the patient did not receive.
  - Notice of insurance benefits (or Explanation of Benefits) for health care services never received.
  - Collection notice from a collection agency for services the patient never received.







THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

### Identity Theft: Your Responsibility

learn about your responsibilities regarding identity theft.




 THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

### Identity Theft: Your Responsibility


learn about your responsibilities regarding identity theft.




**Prevent Identity Theft**  
by keeping patient  
information safe.



**Detect Identity Theft** by being  
aware of suspicious activities.



**Report Identity Theft** as soon as  
you suspect it.


 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

HIPAA stands for Health Insurance Portability and Accountability Act. It is a federal law that requires organizations which provide health care services, such as The Ohio State University, to:

- Follow certain rules when we use and release patient information.
- Keep patient information private, confidential, safe and accurate.

# Health Insurance Portability Accountability Act

 THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

### What is a Hybrid Entity Under HIPAA?


HIPAA allows for large institutions to designate parts that must follow HIPAA called "covered components." This way, only the parts of the institution that meet certain criteria must follow HIPAA.

At The Ohio State University, only the designated health care components and a few other areas must follow HIPAA. In this training, we refer to these special units as "the University." These health care components include:

- The Medical Center,
- OSUP,
- College of Dentistry,
- College of Optometry,
- and others.



**i** If you work in a health care component of the University, you help a covered component do their work, you perform research using information from a covered component, or you have access to protected health information from a covered component, this training applies to YOU.

 THE OHIO STATE UNIVERSITY

<http://compliance.osu.edu/HIPAAprivacyITsecurity.pdf>



Menu | Resources | Contacts


## HIPAA Privacy

We must protect an individual's **Protected Health Information (PHI)** that is:


- Created
- Maintained
- Filed
- Used
- Shared

And is:


**Written**




**Spoken**



**Electronic**



 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts


## HIPAA and Patients' Rights

Patients have the right to:

- Review and request a copy of their own medical and billing records
- Ask for an amendment to their records
- Receive a paper copy of the notice of privacy practices
- Review an accounting of disclosures
- Request a restriction on how their PHI is used or disclosed

**Examples of Protected Health Information (PHI) are:**

- A patient's name, address, birth date, age, phone and fax numbers, e-mail address
- Medical record numbers
- Medical records, diagnoses, x-rays, photos, prescriptions, lab work and test results
- Billing records, claim data, referral authorizations and explanation of benefits
- Certain research records
- Identifiable patient photos (i.e., photos that include the patient's face)

 THE OHIO STATE UNIVERSITY


[Menu](#) | [Resources](#) | [Contacts](#)

## Recent Changes to HIPAA

In 2013, the HIPAA laws changed. Be informed of the changes.

There were many changes to the HIPAA laws in 2013:

- The university must now honor a patient's request for us to restrict information that goes to their insurance company if the patient has paid out of pocket in full for their care.
- OSUWMC updated its Notice of Privacy Practices to comply with the new laws. Check-out the new NPP here: [Joint Notice of Privacy Practices](#).
  - Please contact your privacy officer for specific information regarding the Notice of Privacy Practices for your unit.
- The university updated its business associate agreements.
- The university must notify patients in the event of a Reportable Breach.
  - Learn more in this eLearning.

 THE OHIO STATE UNIVERSITY

To learn more about changes to HIPAA, contact Privacy Officers at:

OSUP/FGP: (614) 685-1530

OSUHS & COM: (614) 293-4477

OSU Health Plan: (614) 292-2542

Nisonger Center: (614) 688-8544

College of Dentistry: (614) 292-6983

College of Optometry: (614) 247-6190

Wilce Student Health: (614) 688-3628

**For additional contact information, click on the Privacy and IT Security Contacts button.**

[Privacy and IT Security Contacts](#)

[Menu](#) | [Resources](#) | [Contacts](#)


## Patient Authorization

There is one key point to remember about releasing protected health information:

**Releasing Protected Health Information Requires Patient Authorization.**

There are a few exceptions to this rule. Authorized staff may disclose information:

- For treatment, payment, or health care operations.
- To fulfill public health reporting requirements to governmental agencies as required by state, federal or local law.
- For law enforcement requests or for purposes other than listed here:
  - OSUHS & COM: Medical Information Management and/or Legal Services must approve the release of information.
  - OSUP/FGP: The Privacy Officer must approve the release of information.
  - The applicable Privacy Officer, in consultation with the Offices of Legal Affairs and/or University Compliance and Integrity as appropriate, must approve the release of information.
- When a Waiver of HIPAA Authorization has been obtained for research purposes.





Menu | Resources | Contacts

### Accounting of Disclosures

Disclosures made without patient authorization that were not for treatment, payment or health care operations, but are otherwise permitted under HIPAA must be accounted for (for example, in OSUWMC's eAccounting or Quick Disclosures systems).

#### Remember to Account for Disclosure of Protected Health Information.

Some examples of when you need to account for a disclosure include:

- Reporting **child or adult abuse** and **neglect** to state agencies.
- Reporting **communicable diseases** as required by law to state agencies.
- Releases to a **coroner** or **medical examiner**.
- Reporting **adverse events** or **product defects** to the **FDA**.
- Reporting **vital statistics** to the **Ohio Department of Health**.


For the Health System, eAccounting may be accessed via the Privacy Office website located here: [Privacy](#)

For OSUP/FPP, eAccounting may be accessed via the OSUP intranet website and is located here: [eAccounting](#)

In addition, you may utilize the Quick Disclosures function in IHIS. To learn more about the Quick Disclosures function, contact the Privacy Office at:

OSUP/FGP: 685-1530  
OSUHS & COM: 293-4477


To learn more, contact the appropriate Privacy Officer; contact information located here: [Contact](#)



THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

### Corrective Action

If it is found that you have been misusing data or inappropriately accessing systems, then you will face corrective action up to and including termination.




THE OHIO STATE UNIVERSITY

**i** Remember in an investigation into HIPAA violations, both The Ohio State and you may be subject to civil or even criminal penalties. These penalties may include fines and possible jail time.


Menu | Resources | Contacts

### HIPAA Security and Passwords


A password, along with your Logon ID, is the “key” that protects your identity within information systems. You protect your passwords in the same way that you would protect the key to your home or automobile. Keep your password a secret.

**Ohio State, OSUWMC, and OSUP IT will **NEVER** request your password.**

- You should not share your passwords with anyone, including co-workers, administrative staff, IT staff, physicians, manager/supervisors or strangers.
- Password sharing is a violation of policy.
- You can reset your own MedCenter Logon ID Password using the Password Change Portal on OneSource (OneSource> MyWorkplace> Password Portal).
- You can reset your university password at [my.osu.edu](http://my.osu.edu).





**i** You are responsible for all activity that occurs under your log-in and password. These penalties may include fines and possible jail time.


 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

### Workstations, Laptops, Smart Phones and Tablets

*learn more about university policies regarding workstations and unsupported devices.*

 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

## Workstations, Laptops, Smart Phones and Tablets


*learn more about university policies regarding workstations and unsupported devices.*

**Computers are business tools you may use to access electronic resources required to perform your job.**

- Physical security of computers is vital to protecting sensitive information.
- Computers should be used for business purposes only and NOT for personal gain or inappropriate activities.
- Where appropriate, computers should be locked to a stationary piece of furniture.
- Position the computer monitor so that sensitive information displayed on the screen is not visible to an unauthorized observer.
- Smartphones and tablets must be managed by the OSUWMC / OSUP Mobile Device Management System in order to access the OSUWMC information systems.
- At OSUWMC/OSUP Laptops, including BYOD and department purchased laptops, must be encrypted.
- For the other covered components, no PHI should be stored on a device that is not encrypted.

**For additional contact information, click on the Privacy and IT Security Contacts button.**

Privacy and IT Security Contacts


 THE OHIO STATE UNIVERSITY

<http://compliance.osu.edu/HIPAAprivacyITsecurity.pdf>

Menu | Resources | Contacts

## Workstations, Laptops, Smart Phones and Tablets


*learn more about university policies regarding workstations and unsupported devices.*



**Devices that are NOT registered or supported by a LAN Manager or OSUWMC IT cannot be attached to the OSUWMC network.**

Unsupported devices create vulnerabilities that may lead to virus outbreaks, information exposure, or network performance issues.


If you have a device that you would like to attach to the OSUWMC network, please contact your LAN manager or the OSUWMC IT Help Desk at (614) 293-3861 or the OSUP Help Desk at (614) 784-7812.


 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

## Software

Only software that is appropriately licensed and approved by your IT department should be installed on devices that are connected to the university network.




 THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

## Software


Only software that is appropriately licensed and approved by your IT department should be installed on devices that are connected to the university network.




**Do NOT install any unlicensed software on any computing devices that uses the university network.**



**Do NOT download, install or run peer-to-peer file sharing applications or devices connected to the university network.**



**Use caution when viewing files from friends. Ask the friend if they sent the message before clicking links that install software such as "Viewers" for video content.**

 THE OHIO STATE UNIVERSITY


Menu | Resources | Contacts

## Malicious Software

**Do not** install peer-to-peer file sharing applications (e.g., Kazaa, Morpheus, Napster, Limewire) on university workstations. They are often used to spread malicious software—programs that covertly enter information systems with the intent of compromising the confidentiality, integrity and availability of data, applications or operating systems.

Malicious software also known as viruses, worms, trojans and spyware, can:

- Lead to identity theft and the exposure of sensitive information.
- Be spread as e-mail attachments.
  - If an attachment looks suspicious, then **do not** open it; **delete it!**
- Be spread through Social Networking Sites such as Facebook and MySpace.


THE OHIO STATE UNIVERSITY

**i** Antivirus software is available free to OSUWMC employees. Visit OSUWMC IT Information Security Home Page or OSU Office of Information Technology for more details. For additional information, contact OSUWMC IT, OSUP IT, or [your local security contact](#).

<http://compliance.osu.edu/HIPAAprivacyITSecurity.pdf>


Menu | Resources | Contacts


## Encryption

### What is Encryption?

Encryption is defined as putting data into a secret code so it is unreadable except by authorized users. Encryption uses keys to scramble and unscramble data.


Per OSU and OSUWMC policy all PHI must be encrypted when stored on portable devices such as laptop computers, smart phones and flash drives.





### Encryption and Remote Access

When working remotely, encryption and wireless security should be considered. Information sent via unencrypted wireless networks can be intercepted by unintended recipients.


THE OHIO STATE UNIVERSITY

**i** For additional information on encryption, contact OSUWMC IT, OSUP IT, or [your local security contact](#).

<http://compliance.osu.edu/HIPAAprivacyITSecurity.pdf>


Menu | Resources | Contacts

### OSUWMC Specific Encryption Tools


If you need to send or transmit electronic Protected Health Information outside of the OSUWMC Network to perform your job, data must be encrypted and you must only use approved methods of transmission such as SecureMail or SFTP.

Messages sent and received through the OSUWMC approved email system are scanned for malicious code and for restricted data to protect our patients and OSUWMC's reputation.

For more information on encryption, please contact your LAN manager or the OSUWMC Help Desk at (614) 293-3861 or the OSUP Help Desk at (614) 784-7812.



**i** To send a message securely from the OSUWMC email system to a non-OSUWMC email address, add [SECURE MAIL] to the subject line of your message.

 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts


### Portable Devices

Portable devices such as laptops, flash drives, smart phones and cameras are powerful and convenient business tools. However, they are also highly susceptible to loss and theft.

Unless the portable device is properly encrypted, you must not store sensitive information such as patient data, Social Security numbers, credit card numbers and financial information. At OSUWMC/OSUP ALL laptops carrying PHI or OSUWMC-owned data MUST be encrypted.


For the other covered components, no PHI should be stored on a device that is not encrypted. For additional information, contact your [local security contact](#).

Physically secure all portable devices when left unattended. Examples include a locked office, file cabinet or trunk, or a cable and lock that is secured to a stationary piece of furniture.



**i** Remember:

- Do NOT leave your laptop or tablet unattended.
- Purchase a locking security cable to attach to your laptop around an immovable object to prevent theft.
- Use strong passwords to prevent unauthorized users from accessing your laptop or tablets.

 THE OHIO STATE UNIVERSITY



<http://compliance.osu.edu/HIPAAprivacyITsecurity.pdf>




Menu | Resources | Contacts

## Data Storage

If you store Protected Health Information (PHI) on a smart phone, laptop, computer, tablet, camera, phone or other storage media, you are the "Data Custodian" for the data and are responsible for its security and proper disposal.



THE OHIO STATE UNIVERSITY

**i** For assistance with properly storing and disposing of sensitive information stored on electronic devices, please contact OSUWMC IT, OSUP IT, or your [local security contact](#).

Menu | Resources | Contacts

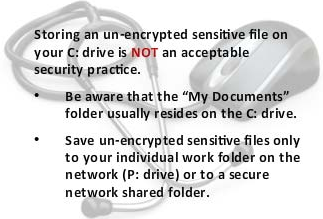
## Data Storage

If you store Protected Health Information (PHI) on a smart phone, laptop, computer, tablet, camera, phone or other storage media, you are the "Data Custodian" for the data and are responsible for its security and proper disposal.

Click each **image** to learn more.


Basic protections require that Data Custodians must:

- Locate the file on a secure department shared (network) drive that is protected from those who do not require access to the data.
- Encrypt (password protect) the data files (MS Office documents).
- Password protect data devices (MS Access).
- Completely destroy the document when it is no longer needed.



Storing an un-encrypted sensitive file on your C: drive is **NOT** an acceptable security practice.

- Be aware that the "My Documents" folder usually resides on the C: drive.
- Save un-encrypted sensitive files only to your individual work folder on the network (P: drive) or to a secure network shared folder.



THE OHIO STATE UNIVERSITY

**i** For assistance with properly storing and disposing of sensitive information stored on electronic devices, please contact OSUWMC IT, OSUP IT, or your [local security contact](#).

<http://compliance.osu.edu/HIPAAprivacyITsecurity.pdf>

### Disclosures to Family and Friends

HIPAA permits a patient's provider to share information with a patient's family and friends involved in the patient's health care or payment for the patient's health care if:

- The patient tells the provider that he or she can do so.
- The patient does not object to sharing the information.
- Using professional judgment, the provider believes that the patient does not object.

Disclosures to family and friends is a tricky topic that warrants more reading.



Access this website here [HERE](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/family-and-friends)

### Minimum Necessary Requirement

HIPAA's minimum necessary standard means that we are only allowed to release the minimum amount of information necessary to accomplish the intended purpose of the release of patient information.

For example, a patient is being discharged from the hospital. The provider talks with the patient's family member about when to give the patient's medication. In this discussion, the provider may only share with the family member the minimum amount of information necessary about that the family member needs to help with the patient's care at discharge. Nothing more.



<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>

## OSUWMC Break The Glass

Break-the-glass is a security feature within IHIS that helps safeguard PHI and assists with privacy auditing.

Break-the-glass (BTG) can be applied in one of two ways:

- At the encounter level – An end user is required to break the glass when opening an encounter with BTG protection.  
Example: Talbot, Harding, Select, NCH
- At the patient level – An end user is required to break the glass when opening a patient record.  
Example: A high profile patient or “person of interest” who has been in the news media and is being treated at OSUWMC.



When an end user attempts to open an encounter or record that is protected with BTG, a warning box will appear:

The end user must enter their username, password, and a reason for entering. The Privacy Office is notified of all attempts at breaking the glass and performs daily audits of the breaks.

- An end user is considered to have “bumped the glass” when he/she receives the warning box above and cancels out, times out, or fails to authenticate with their username/password. Such is the case if an end user searches for a patient, receives the warning box, and then cancels out. The Privacy Office is notified of all “bumps” and includes them in their routine BTG audits.
- If you receive the BTG warning while attempting to perform your job duties, you should feel comfortable breaking the glass.



## Reasonable Safeguards

The university must make it a practice to be sure that we take reasonable safeguards to protect patient information such as:

- Speaking quietly when talking about patients with family members in a waiting room or other public area.
- Avoid using patients' names in public hallways and elevators.
- Isolating or locking file cabinets or rooms containing patient information on paper.





Access this website [HERE](#)

Menu | Resources | Contacts

### Proper Disposal of Trash

- Shred ALL Paper – all paper should be placed in a locked shredding bin. This includes magazines, billing information, and patient information. The Shred-it bin must be locked at all times and key access is limited to Managers only.
- **DO NOT** overstuff Shred-it bins; sensitive documents can be easily retrieved if bins are completely full.
- **DO NOT** place paperwork containing PHI in a “shred box” on your desk or in a blue recycling bin under your desk. Promptly discard all paperwork in Shred-it bins.
- Email [secure shredding@osumc.edu](mailto:secure shredding@osumc.edu) or call your local facilities representative with questions about shredding.



 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

### Marketing and Fundraising

**Question:**  
I want to mail out letters to previous patients of the university to inform them of a new procedure being offered at the Ross Heart Hospital. Can I send the letter to previous patients of the university without receiving authorization from the patients?

**Answer:**  
It depends on whether the letter is for the purpose of **marketing** or **fundraising**.

<p>If the purpose of the letter falls within the definition of <b>“marketing,”</b> a signed authorization must be obtained from the patient, unless an exception applies. If one of the following exceptions apply, a signed authorization is NOT necessary:</p> <ul style="list-style-type: none"> <li>• Communication about the university’s own products or services.</li> <li>• Communication made for the Treatment of the Individual.</li> <li>• Communication made for Case Management or Care Coordination of a patient.</li> <li>• Face-to-Face Marketing Communication.</li> </ul>	<p>If the purpose of the letter falls within the definition of <b>“fundraising,”</b> the university may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without authorization:</p> <ul style="list-style-type: none"> <li>• Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth.</li> <li>• Dates of health care provided to an individual.</li> <li>• Department of service information.</li> <li>• Outcome information.</li> <li>• Health Insurance Status.</li> </ul>
--	--

In addition, the university must state its Notice of Privacy Practices, the possible uses, and disclosures of PHI for fundraising purposes. The university must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The university may NOT make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications .

Menu | Resources | Contacts

## HIPAA Breach Notification Rules

In 2009, the American Recovery and Reinvestment Act of 2009 (ARRA) brought changes to HIPAA.


The [Breach Notification Provisions](#) is one change to HIPAA. Take a moment to review these changes.

If you suspect a breach has occurred, please contact Privacy Officers at:

- OSUP/FGP: (614) 685-1530
- OSUHS & COM: (614) 293-4477
- OSU Health Plan: (614) 292-2542
- Nisonger Center: (614) 688-8544
- College of Dentistry: (614) 292-6983
- College of Optometry: (614) 247-6190
- Wilce Student Health: (614) 688-3628

**Breach Notification Provisions:**

- Where there is a Breach of patient information as defined by the regulation (a Reportable Breach), the university **must notify the patient**.
- For Reportable Breaches involving more than 500 patients, the university must also notify the press.
- For all Reportable Breaches, the university must notify the Department of Health and Human Services, Office for Civil Rights.

 THE OHIO STATE UNIVERSITY


**Breach Notification Provision:** [HERE](#)  
**Privacy and IT Security Contacts:** [HERE](#)


Menu | Resources | Contacts

## Summary

To summarize what you've learned:

- Under new HIPAA laws we must notify patients and the federal government when we have a breach of patient information.
- Inappropriate access to patient information qualifies as a Breach under the new laws.
- You must do all you can to keep patient information secure.


 THE OHIO STATE UNIVERSITY



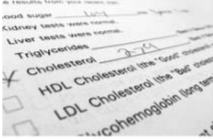
Menu | Resources | Contacts

## HIPAA Violation Scenarios


The following icons identify common areas of HIPAA violation.




**Suspicious Behavior**




**Checking Patient Information**




**Paper Handling of PHI**




**Electronic Handling of PHI**




**Securing PHI on Devices**



**Criminal Activity**




**Reporting Breach of PHI**

 THE OHIO STATE UNIVERSITY

## Suspicious Behavior Scenarios

HIPAA Violation Scenarios

Scenario	What is Wrong	What to Do
<b>Duplicate Social Security Number (SSN)</b> You have access to the electronic medical record. You search by patient name and date of birth. Two patients return with the same SSN, but with different birth dates.	Two patients with the same SSN is an Identity Theft Red Flag.	<b>Take one of the following actions:</b> <ul style="list-style-type: none"> <li>Notify your manager who will complete an initial investigation. If your manager is unavailable, then notify the Privacy Office:</li> <li>OSU Physicians, Inc. (OSUP) and Faculty Practice Group (FGP): (614) 685-1530</li> <li>OSU Health System (OSUHS) &amp; College of Medicine (COM): (614) 293-4477</li> <li>File an anonymous complaint via the Ethics Point Reporting System</li> </ul> OSUP/FGP: 1-800-559-5217 FREE <a href="https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=14670">https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=14670</a> OSUHS & COM: 1-866-294-9350 FREE <a href="https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7689">https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7689</a> The Identity Theft Red Flag Rules Response Team will investigate the situation.
<b>Colleague's Suspicious Behavior</b> Your colleague has access to patient and staff SSNs. Recently, you notice that your colleague is placing stacks of papers in envelopes and sending them out in the mail or taking the information home. This is not something your colleague needs to do as part of her job duties.	Your colleague's behavior is an Identity Theft Red Flag. The worst case scenario is that your colleague is stealing patient information and selling it for misuse by identity thieves. This type of theft has occurred at other hospitals.	

 THE OHIO STATE UNIVERSITY



## Checking Patient Information Scenarios

### HIPAA Violation Scenarios

Scenario	What is Wrong	What to Do
<b>Reviewing Family Member Records</b> You are helping to provide care for your family member by taking them to doctor appointments and helping them at home. You are also listed as your family member's emergency contact. You have no job-related responsibilities to care for this family member. You are curious about the results of your family member's recent lab results. You log into the electronic medical record just to see if your family member's test results have been completed.	You did not need to access your family member's record for a job-related reason.  Looking up this information may be a violation of hospital policy and may be a violation of state and federal laws.	You must only access patient information as needed to perform your job duties. Failure to do so will result in corrective action up to and including termination. Access to patient information is monitored. You are responsible for all that occurs under your login and password. If you have any questions about whether access to patient information is appropriate, ask your supervisor and/or contact: <ul style="list-style-type: none"> <li>• OSUP/FGP: (614) 685-1530</li> <li>• OSUHS &amp; COM: (614) 293-4477</li> <li>• OSU Health Plan: (614) 292-2542</li> <li>• Nisonger Center: (614) 688-8544</li> <li>• College of Dentistry: (614) 292-6983</li> <li>• College of Optometry: (614) 247-6190</li> <li>• Wilce Student Health: (614) 688-3628</li> <li>• <a href="#">Your Local Privacy Office</a>.</li> </ul>
<b>Checking Patient Information When Not in Your Care</b> You are watching the football game and see that a Famous Football Player has been injured. You think that he is being treated at OSUWMC, but you are not sure. You are NOT involved in the Famous Football Player's care.  You have access to patient information. You log into the electronic medical record just to check if the Famous Football Player has been admitted to OSUWMC for treatment.	You did not need to know whether Famous Football Player was admitted to the hospital to perform your job.  Looking up this information is a violation of hospital policy and may be a violation of state and federal laws.	

## Paper Handling PHI Scenarios

Scenario	What is Wrong	What to do
<b>Removing PHI on Paper from University Premises</b> Resident Rita prints a rounds report and leaves it in the pocket of her white coat. At the end of the day while leaving the hospital the list falls out of her pocket onto the sidewalk.	Rita inappropriately took PHI from the hospital, exposing the information to risks of loss or theft. PHI on paper is easily lost or stolen and you are responsible for ensuring that it remains secure by properly disposing of the information when it is no longer needed. Rita should have properly disposed of the information before leaving the hospital.  Inappropriately removing information from the hospital could result in corrective action up to and including termination.	PHI must be kept secure at all times. Whenever possible, medical record information should be accessed electronically and paper record transport kept to a minimum. Medical record documents are to be stored at all times at university sites. If you have questions about PHI on paper and how to properly secure it or dispose of it, ask your supervisor and/or contact: <ul style="list-style-type: none"> <li>• OSUP/FGP: (614) 685-1530</li> <li>• OSUHS &amp; COM: (614) 293-4477</li> <li>• OSU Health Plan: (614) 292-2542</li> <li>• Nisonger Center: (614) 688-8544</li> <li>• College of Dentistry: (614) 292-6983</li> <li>• College of Optometry: (614) 247-6190</li> <li>• Wilce Student Health: (614) 688-3628</li> <li>• <a href="#">Your Local Privacy Office</a>.</li> </ul>
<b>Securing PHI Paperwork</b> You are a medical secretary who supports a doctor who sees patients at multiple sites. You carry paper medical records and patient documents to the sites. At the end of the day, you take them home with you.	It is a dangerous practice to transport medical records yourself. You are responsible for the security of the information when it is in your possession. Paper medical record transport between university sites should be handled by dedicated medical record couriers.	

[More Scenarios](#)

### Paper Handling PHI Scenarios (cont ...)

Scenario	What is Wrong	What to Do
<b>Fax Machines and Printers</b> The clinic has a fax machine and printer located in a patient waiting area. These machines are often unattended and receive faxes and print jobs containing PHI throughout the day and night.	The clinic has the fax/printer located in an unsecure location. The machines are unattended while receiving print jobs and faxes.	Fax machines and printers that receive PHI must be kept in a secure area. They must be accessible and attended to only by authorized university staff. PHI sent to these machines must be removed promptly.  If you have questions about faxing or printing PHI and how to properly secure it, ask your supervisor and/or contact the <a href="#">Privacy Office</a> .
<b>Patient Addresses, Zip Codes and Medical Record Numbers</b> As part of Andrew's job, he prints out information that includes patient addresses and zip codes. He thinks that he should place these documents in the shredder bin, but whenever he goes there, it is either full or unlocked. Andrew decides that because there is no patient name on the papers, that it is okay to throw the papers in the regular trash.	Patient addresses, zip codes, and medical record numbers are Protected Health Information even if there are no patient names on the papers.	Place paper with PHI and any sensitive information in a shredding container.  Where paper is kept in a box under your desk to be emptied into a shredding bin, you must empty the box at the end of each day into a shredding bin and mark the box as "Shredding – Do Not Throw in the Regular Trash." If the shredding container in your area is full or unlocked, notify: <ul style="list-style-type: none"> <li>• OSUHS: Environmental Services (614) 293-8645 / (614) 293-4230</li> <li>• OSUP/FGP: (614) 685-1530</li> <li>• OSUHS &amp; COM: (614) 293-4477</li> <li>• OSU Health Plan: (614) 292-2542</li> <li>• Nisonger Center: (614) 688-8544</li> <li>• College of Dentistry: (614) 292-6983</li> <li>• College of Optometry: (614) 247-6190</li> <li>• Wilce Student Health: (614) 688-3628</li> <li>• <a href="#">Your Local Privacy Office</a>.</li> </ul>

[More Scenarios](#)

### Paper Handling PHI Scenarios (cont ...)

learn what to do in those situations before proceeding to the next page.

Scenario	What is Wrong	What to Do
You are a PCA who checks out patients. Part of this check out includes printing a copy of the AVS for the visit and handing it to the patient. You forget to give the previous patient (Patient A) her After Visit Summary (AVS) and include it with the AVS printed and given to Patient B.	When providing Protected Health Information to a patient, you are responsible for ensuring the information being provided to each patient is correct. Each page should be confirmed prior to providing the information to the patient.	If you are contacted by a patient who has received another patient's information in error, ask the patient to hold the information. Send this patient a self-addressed, stamped envelope to return the information back to us. Also include an Attestation form to the patient to sign that states while the information was in possession, it was not used or disclosed in any way. Explain all of this to the patient before mailing the form/envelope. If you have any questions, contact the <a href="#">Privacy Office</a> .

## Electronic Handling of PHI Scenarios

Scenario	What is Wrong	What to Do
<b>Social Media</b> You mention on your Facebook page that you saw your favorite restaurant owner today in the clinic where you work.	Information about patients must not be posted to any social media site, including but not limited to blogs, wikis, instant messaging, email outside of the university, social networks and video-hosting sites.	With the use of social media, you are responsible for protecting our patients and yourself every day. If you have questions about the proper use of social media, consult the Medical Center's social media policy and/or contact the <a href="#">Privacy Office</a> .
<b>Phishing Attempts</b> You receive an email from IT Support stating that OSUWMC is performing system maintenance and telling you to provide your User ID and password.	Phishing is where people send an email to a user falsely claiming to be a legitimate requestor. Phishing tries to scam a user into surrendering private information. The university IT will NEVER request your password.	If you receive suspected phishing e-mail, please report it to <a href="mailto:report-phish@osu.edu">report-phish@osu.edu</a> . If in doubt as to the legitimacy of an e-mail, before taking any action, please contact your local IT support, the IT Service Desk at (614) 688-HELP (4357), the OSUWMC IT Help Desk at (614) 293-3861, or the OSUP Help Desk at (614) 784-7812 for verification and advice.
<b>Sharing Passwords</b> You are working with a new staff member that doesn't currently have access to log into the computer. You need the staff member's assistance. You log into the electronic medical record and allow the staff member to use your account to access PHI.	Both staff members violated policy. You are responsible for all activity that occurs under your login and password.	Do NOT share your passwords with anyone. Password sharing is a violation of policy. Violations of policy may result in corrective action up to and including termination. If your manager or supervisor asks you to share your password with a new employee, tell them this is not permissible per HIPAA Security rules and internal policies. If they still insist, contact the HIPAA Privacy Officer. If you have questions about computer access to PHI, ask your supervisor or contact your local IT support, the IT Service Desk, OSUWMC IT Help Desk, or OSUP Help Desk.

## Securing PHI on Devices Scenarios

### PHI Violation Scenarios

Scenario	What is Wrong	What to Do
<b>Equipment Registration</b> Researcher Ron is recruited to do research with the Medical Center. Ron hires a research assistant that has some computer skills and asks that she set up and maintain some non-medical center owned computer equipment that is needed for his study.	Researcher Ron's assistant is not a LAN manager and is not part of OSUWMC IT. Therefore, she is not authorized to maintain and support equipment attached to the OSUWMC network. Computer equipment that is not properly maintained may lead to virus outbreaks, information exposure and network performance issues.	Devices that are NOT registered and supported by a LAN manager or OSUWMC IT cannot be attached to the OSUWMC network. If you have questions about attaching computers to the OSUWMC network or accessing OSUWMC applications using non-OSUWMC issued devices, ask your supervisor and/or contact the OSUWMC IT Help Desk: (614) 293-3861.
<b>Installing Software</b> It's the Holiday season and you receive a message in your Social Networking account to view a funny video from a friend. When you click on the link in the message, you are prompted to install a viewer before you can watch the video.	Installing unauthorized software can introduce a virus or malicious code into the university computer network and compromise sensitive information.	STOP! Delete the email!

[More Scenarios](#)

### Securing PHI on Devices Scenarios (cont...)

Scenario	What is Wrong	What to Do
<b>PHI Data Storage</b> Bill and Carla are sharing a spreadsheet to analyze patient outcomes. The spreadsheet is stored on a Secure department shared drive. Carla decides to create her own copy of the spreadsheet on her desktop.	Carla is placing the data on her C: drive which is an unsafe place for patient information.	Patient information must be saved to a folder on the network (P: drive) or to a secure network shared folder. If you need assistance with properly storing and disposing of sensitive information, contact your local IT support, the IT Service Desk at (614) 688-HELP (4357), your LAN manager, or the OSUWMC Help Desk (614) 293-3861 or the OSUP Help Desk (614) 784-7812.
<b>Storing PHI on Portable Devices</b> Nurse Neal received the latest smart phone as a birthday present. He would like to use the device to access his university email and clinical applications.	Devices such as laptops, smartphones and flash drives are easily lost or stolen. They must be encrypted to protect restricted data such as PHI per OSU and OSUWMC policy.	Contact your local IT support or OSUWMC IT to have the device properly encrypted and secured before accessing the university's electronic resources. If you have questions about storing PHI or other restricted data on portable devices, ask your supervisor and/or contact your local IT support, the IT Service Desk at (614) 688-HELP (4357), your supervisor, or the OSUWMC Help Desk (614) 293-3861 or the OSUP Help Desk (614) 784-7812.
<b>Encryption of PHI</b> Doctor Jones uses her personal flash drive to store information about her patients. The drive is not encrypted. One day during her rounds she mistakenly leaves the flash drive on a nursing unit and is unable to find it when she returns.	Dr. Jones was using an unsecured flash drive to store PHI. Portable equipment is easily lost or stolen and must be encrypted in order to protect restricted data such as PHI.	Per OSU and OSUWMC policy, all PHI must be encrypted when stored on portable devices such as laptop computers, smart phones and flash drives. If you have questions about encrypting PHI on portable devices, ask your supervisor and/or contact your local IT support, the IT Service Desk at (614) 688-HELP (4357), your supervisor, or the OSUWMC Help Desk (614) 293-3861 or the OSUP Help Desk (614) 784-7812.

### Criminal Activity Scenarios

#### PAA Violation Scenarios

Scenario	What is Wrong	What to Do
<b>Releasing Patient Information for a Criminal Investigation</b> You recognize a patient you are taking care of as a suspect in a criminal investigation. You know he is a suspect because you remember seeing him on the news a few nights ago. You want to help by calling the police and letting them know that the suspect is a patient at university.	<b>Stop!</b> You may do more harm than good by releasing information inappropriately. Releasing patient information without signed patient authorization could be a violation of federal HIPAA laws and multiple state laws.	Giving out patient information in violation of hospital policies will subject you to corrective action up to and including termination. Where there is a reportable breach of patient information under HIPAA regulations, we must notify the patient in writing of the breach and notify the federal government as well. OSUWMC employees should call Legal Services, Risk Management (page 2001) and others should call their Privacy Officer and the Office of Legal Affairs to ask for help before releasing information in these situations.
<b>Patient Assault on Another Patient</b> Your patient was involved in an assault of another patient while in the hospital. Your patient has several diagnoses including an arrhythmia, hypertension and depression. The police come to the patient's room to investigate the assault. The police officer asks you about the situation.		

## Reporting Breach of PHI Scenarios

### HIPAA Violation Scenarios

Scenario	What is Wrong	What to Do
<b>Reporting Breach of PHI</b> Dr. Holland was watching news reports about a prominent local news anchor who was involved in a severe car crash. He noticed that the news anchor was admitted to the hospital where he works. Dr. Holland logged onto the hospital's medical record to see if the news reports were true. Dr. Holland was not involved in the news anchor's care. Out of curiosity, Sarah, a registration clerk, and Carmen, a clinic nurse, also viewed the patient's medical record.	Dr. Holland, Sarah and Carmen did <b>NOT</b> need this information to do their jobs. Their curiosity may be considered a <b>Breach</b> under the new regulations.	The university must assess all potential breaches of its PHI. All reportable breaches must be reported to the Federal Government annually. When a situation like this occurs, the university must also write a letter to the patient to tell the patient: <ul style="list-style-type: none"> <li>• Her information has been breached.</li> <li>• The date and time of the breach.</li> <li>• What the university has done to prevent future incidences.</li> <li>• Contact information about where she can get further information.</li> </ul>
<b>Misdirected Email Containing PHI</b> Jennifer Smith receives an email from Dr. Donna. Jennifer often receives misdirected emails because there are at least four other Jennifer Smiths that work at the university. Jennifer notices that she is not the intended recipient of Dr. Donna's email. Jennifer Smith works in a lab at the College of Medicine and does not use patient information to do her job.	Patient information is in the wrong hands and could be compromised.	

[More Scenarios](#)

Scenario	What is Wrong	What to Do
<b>Lost Flash Drive Containing PHI</b> Terry lost his flash drive a few days ago. Terry kept patient information on the flash drive, including patient names, admission dates, copies of patient prescriptions and clinic patient lists. Terry didn't notify anyone that his flash drive was lost because he thought it would turn up some day. Over two weeks has past and Terry has not located his lost flash drive.	Terry should not store PHI unless it has been encrypted. He should have notified the Privacy Officer about the lost device ASAP after noticing it was lost.	Do not store PHI on devices unless it is encrypted. If a device with PHI on it is lost, notify the Privacy Officer ASAP: <ul style="list-style-type: none"> <li>• OSUP/FGP: (614) 685-1530</li> <li>• OSUHS &amp; COM: (614) 293-4477</li> <li>• OSU Health Plan: (614) 292-2542</li> <li>• Nisonger Center: (614) 688-8544</li> <li>• College of Dentistry: (614) 292-6983</li> <li>• College of Optometry: (614) 247-6190</li> <li>• Wilce Student Health: (614) 688-3628</li> <li>• <a href="#">Your Local Privacy Office</a>.</li> </ul> <p>The clock is ticking! Once the employee discovers a potential breach, the university has no more than 60 days to notify the patients of the Breach.</p>
<b>Papers Found Containing PHI</b> Joe is a faculty member at the College of Medicine and works primarily in a research lab. He meets his friend for lunch at the hospital cafeteria. When Joe sits down, he finds papers on the cafeteria table. On the papers, he sees a list of patient names with notes about each patient.	PHI might have been compromised and needs to be returned to the Privacy Office.	If you find papers with PHI on them, notify the Privacy Office ASAP. The Privacy Office will ask you to return the information ASAP, investigate further, and present the investigation to the potential breach committee to determine the likelihood that the data has been compromised.

[Menu](#)
[Resources](#)
[Contacts](#)

### Common Questions

Does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

May a health care provider discuss a patient's health information over the phone with a family member, friend, or others involved in the patient's care or payment for the patient's care?

How should the university employees protect paper documents that contain sensitive information about our staff, patients and vendors?

What if patients or family members overhear us talking about other patients in a shared or open patient care setting?


**Answer #1**

If the patient is present and has the capacity to make health care decisions, then a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object.

A health care provider may share information with these persons if, using professional judgment, the provider decides that the patient does not object.

In either case, the health care provider may share or discuss **ONLY** the information that the person involved needs to know about the patient's care or payment for care.

- If there is a frequent visitor in the room when the physician (or other staff) comes in, the health care provider should ask the patient (or the patient's legal representative) if a private conversation is preferable.
- Use professional judgment, but make it comfortable for the patient to say: "I'd like to keep this discussion private."


THE OHIO STATE UNIVERSITY

[Menu](#)
[Resources](#)
[Contacts](#)

### Common Questions

Does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

May a health care provider discuss a patient's health information over the phone with a family member, friend, or others involved in the patient's care or payment for the patient's care?

How should the university employees protect paper documents that contain sensitive information about our staff, patients and vendors?

What if patients or family members overhear us talking about other patients in a shared or open patient care setting?


**Answer #2**

Yes. Where a health care provider is allowed to share a patient's health information in-person, information may be shared over the phone as well.

However, **proceed with caution:**

- If the patient has asked you not to share information with a family member, then you must not share the information.
- If you are uncertain whether the patient would want you to, then do not share the information.
- If you are uncertain of the identity of the caller, then do not share the information.

If you work in the hospital, know your unit's policy. Many units use code numbers or words that signal to staff that the caller has been identified as someone with whom you may share information.


THE OHIO STATE UNIVERSITY



Menu | Resources | Contacts

## Common Questions

Does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

May a health care provider discuss a patient's health information over the phone with a family member, friend, or others involved in the patient's care or payment for the patient's care?


**How should the university employees protect paper documents that contain sensitive information about our staff, patients and vendors?**

What if patients or family members overhear us talking about other patients in a shared or open patient care setting?

**Answer #3**

Documents that contain sensitive information such as patient information should be maintained behind a **locked door** to which other staff do not have access after hours.

If other staff have access to your desk after hours, then sensitive information must be placed in a **locked drawer**.

 THE OHIO STATE UNIVERSITY

Menu | Resources | Contacts

## Common Questions

Does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

May a health care provider discuss a patient's health information over the phone with a family member, friend, or others involved in the patient's care or payment for the patient's care?


How should the university employees protect paper documents that contain sensitive information about our staff, patients and vendors?

**What if patients or family members overhear us talking about other patients in a shared or open patient care setting?**

**Answer #4**

In shared or open patient care settings, use reasonable safeguards to make sure that the patient's privacy rights are respected:

- Monitor the volume of your conversation and pull curtains whenever possible.
- When sharing sensitive results or discussing sensitive information with patients, offer a private setting whenever possible.
- Don't talk about patients in elevators, the cafeteria, or other public places.

 THE OHIO STATE UNIVERSITY


Menu Resources Contacts


**Conclusion**

**You have completed Annual HIPAA Privacy & Security.**

**After reviewing this course, you should now be familiar with:**

- Recognizing that privacy and Security of sensitive information is your responsibility
- Identifying situations where sensitive information may be handled improperly
- How you can protect patient and confidential information in common workplace situations
- Recognizing that you will be held responsible for improperly handling sensitive information
- Determining who to notify if you have questions about the privacy and security of sensitive information

A group of approximately ten healthcare professionals, including nurses and doctors, are posed for a group photo. They are wearing various shades of blue and green scrubs. Some are standing in the front row, while others are slightly behind them. They are all smiling and looking towards the camera.

 THE OHIO STATE UNIVERSITY