



Contingent Worker Offsite Training

Version

OF.01

HIPAA/HITECH.....Page 2

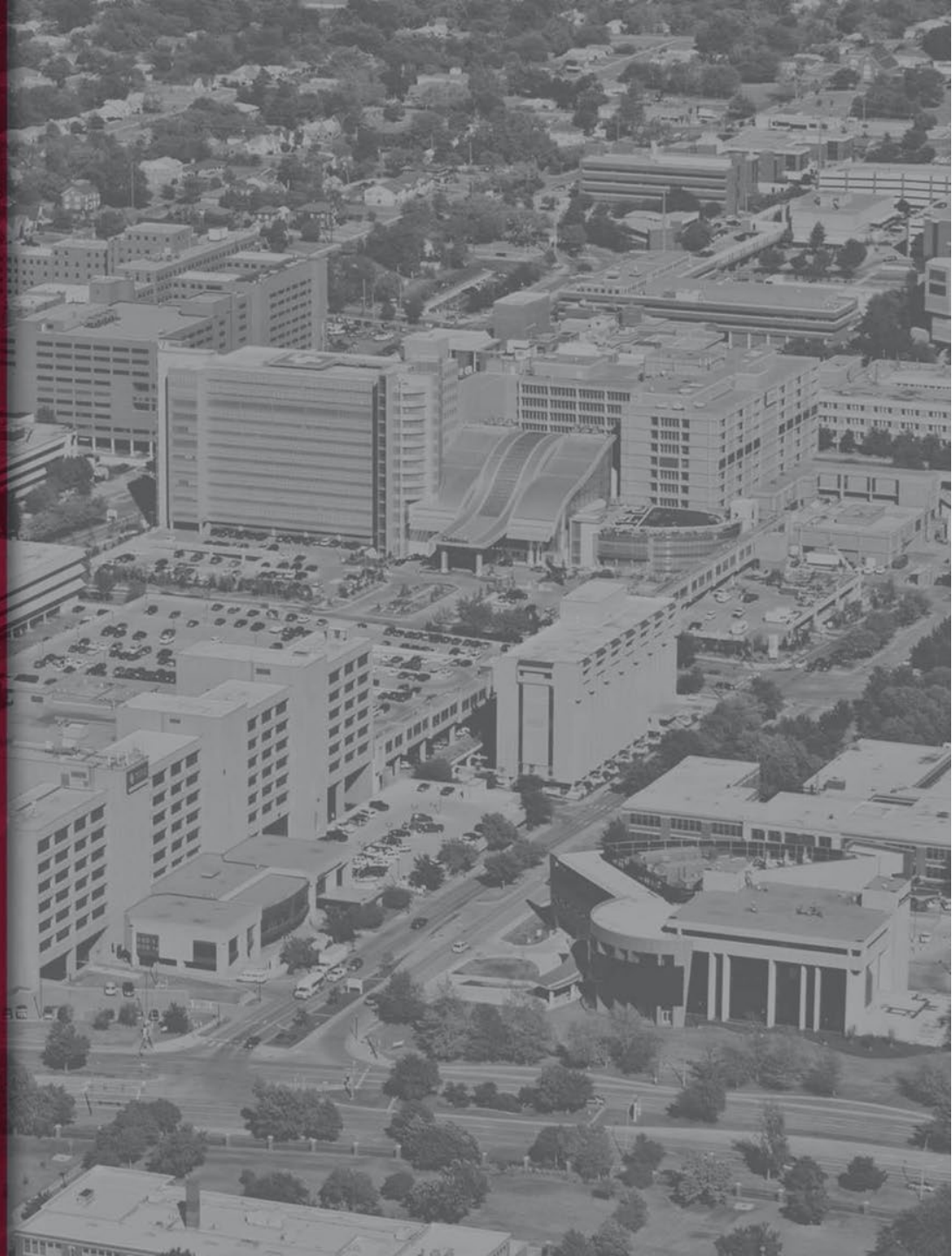
Code of Conduct.....Page 37



Medicine

HIPAA/HITECH Training

Administrative Staff



Objectives

Participants will be able to:

- Describe an overview of HIPAA and HITECH privacy key definitions and principles
- Describe how HIPAA and HITECH affect job duties
- List tips and guidance for applying privacy requirements

HIPAA Terminology

- BAA: Business Associate Agreement
- HIPAA: Health Insurance Portability and Accountability Act
- HITECH: Health Information Technology for Economic and Clinical Health Act
- PHI: Protected Health Information
- CE: Covered Entity (Hospital, physician practice, surgery center)
- ACE: Affiliated Covered Entity (Common ownership)
- OHCA: Organized Health Care Arrangement (The hospital and medical staff will be considered an Organized Health Care Arrangement)
- DRS: Designated Record Set (medical record and billing record)
- AOD: Accounting of Disclosures (patient's right to receive)
- Directory: Hospital census list used by volunteers and operators with name and room

Hospitals are required by law to maintain the privacy of patients' health information.

It is everyone's responsibility to ensure patient information is properly protected and safeguarded!



Facility Privacy Official (FPO)

What is a FPO?

- The FPO is the “go-to” person for any
Potential patient privacy issues
Questions on patient privacy matters
Patient privacy questions and complaints
- The FPO oversees and facilitates the privacy program
including all training and compliance
- FPO for OU Medicine is Amber Simpson

HIPAA Definition & Purpose

What is HIPAA?

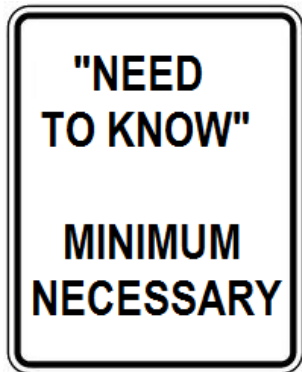
- The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
- Mandatory federal law.

What is the purpose of the law?

- Protect health insurance coverage, improve access to healthcare
- Reduce fraud, abuse and administrative health care costs
- Improve quality of healthcare in general

How does HIPAA affect you?

- Business Associate Agreements must be obtained on all contracts where they are performing a service on the facility behalf and PHI is exchanged.
- Patient information should only be accessed if there is a need to know (e.g., the information is required for the treatment of a patient, to carry out health care operations or for payment purposes). Only the minimum necessary amount of information may be used.
- All workforce members must have privacy job specific training.



How does HIPAA affect you? Cont.

- Reasonable safeguards must be put into place for patient privacy protection.
- Patients are provided with their privacy rights at the time of admission/registration via a Notice of Privacy Practices.
- Written patient authorization is required for disclosures that are not related to treatment, payment, or healthcare operations (TPO).

What is Protected by HIPAA?

PHI is the information pertaining to healthcare that contains any of these identifiers. People often believe that if the patient's name is removed then the information is not PHI. That is not true. There are many types of patient identifying information.

- Name
- Address including street, county, zip code and equivalent geocodes
- Name of relatives
- Name of employers
- All elements of dates except year (DOB, admission/ discharge, expiration, etc.)
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security number
- Any vehicle or other device serial number
- Medical Record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any other unique identifying number, characteristic or code
- Web universal resource locator (URL)
- Internet protocol address (IP)
- Finger or voice prints
- Photographic images



HITECH Definition & Purpose

What is HITECH?

- The Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law by the President on February 17, 2009. It is the part of the American Recovery and Reinvestment Act (ARRA) of 2009.
- It is a federal law.
- HITECH Act strengthens those patient privacy protections of HIPAA and places additional requirements on the healthcare community.

What is the purpose of the law?

- Makes massive changes to existing privacy and security laws
- Applies to covered entities and business associates
- Increases penalties for privacy and security violations
- Creates a nationwide electronic health record



Key HITECH Changes

While there are many changes as a result of HITECH, some of the more substantial changes include:

- Breach Notification
- Penalties
- Criminal provisions
- Accounting of Disclosure for treatment, and health care operations in electronic health record (EHR) environment
- Business Associate Agreements
- Right to Access
- Restrictions
- OCR Privacy Audits
- Copy charges for providing copies from EHR
- Sharing of civil monetary penalties with harmed individuals
- Private cause of action
- HIPAA preemption applies to new provisions

Let's look at some of the details of these changes.



Breach Notification

A breach is any impermissible acquisition, access, use, or disclosure of unsecured protected health information which compromises the security or privacy of such information.

HITECH provisions requires the following notifications when breaches (as defined in PHI.006) occur:

- To the patient
- To the Department of Health and Human Services
- To the media when the breach involves more than 500 Individuals in the same state or jurisdiction

Civil Monetary Penalties for Non-Compliance*

Violation Category	Each Violation	All such violations of an identical provision in a calendar year
Did not know	\$110 - \$55,010	\$1,650,300
Reasonable Cause	\$1,100 - \$55,010	\$1,650,300
Willful Neglect – Corrected	\$11,002 - \$55,010	\$1,650,300
Willful Neglect – Not Corrected	\$55,010	\$1,650,300

*As of 9/06/2016

Criminal Penalties for Non-Compliance

- For health plans, providers, employees, clearinghouses and business associates that knowingly and improperly disclose information or obtain information under false pretenses can be assess penalties. These penalties can also apply to any “person”.
 - up to \$50,000 and one year in prison for obtaining or disclosing protected health information (PHI)
 - up to \$100,000 and up to five years in prison for obtaining protected health information under "false pretenses"
 - up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm
- Penalties are higher for actions designed to generate monetary gain.



What is a Covered Entity (CE)?

- A Covered Entity is any entity that is subject to HIPAA and HITECH
- Health plans, health care clearing houses, and health care providers that transmit electronically for billing:
 - Hospitals
 - Physician Practices
 - Insurance Companies
 - Ambulance transportation services
 - Home Health Agencies
 - Hospice

What is a Business Associate (BA)?

- A person, company, corporation or any other legal entity that creates, receives or uses PHI to perform a function or activity on behalf of the facility or to perform certain professional services for the facility, such as:

Billing

Legal

Quality Assurance

Claims Processing

Contracts

- Must be identified for all departments
- An OUM HITECH-compliant Business Associate Agreement (BAA) must be executed if PHI will be created, received, maintained, or transmitted
- Facility must maintain a listing of BAAs

Patient's Right to Access


- Patients have a right to inspect or obtain copies of their medical and billing records
- Facility will provide a readable hard copy of portions of the record requested
- Must provide access within 30 days (or an additional 30 days if stored offsite)

For More Information Review:

PHI.032 Patient's Right to Access



Patient's Right to Amend


OU Medical Center | The Children's Hospital | OU Medical Center Edmond | Breast Health Network

Request for Amendment of Health Information

Patient Information:	
Patient Full Legal Name:	Date of Request:
Legal Guardian's Name (if applicable):	Patient's Birthdate:
Patient Account/Medical Record #:	Phone Number: ()
Street Address:	
City, State, Zip:	Email Address:
Summary of Request:	
Describe the information you would like amended (e.g. lab test results, physician notes) *Please attach additional pages if more space is needed	
Provide the date(s) of the information to be amended (e.g., date of office visit, treatment, or other health care service)	
What is your reason for making this request?	
How is the entry incorrect or incomplete?	
Do you know of anyone who may have received or relied on the information in question such as your doctor, pharmacist, health plan, or other health care provider? (Circle one) YES NO	
If yes, please specify the name(s) and address(es) of the organization(s) or individual(s):	
If the amendment is accepted, do we have your permission to share the amendment with individuals listed who have received this information? (Circle one) YES NO	
Attachments:	
Required:	Attach a copy of the record that you are requesting be amended. Please make notes on the attached copy that identify the changes you are requesting be made to the record.
Signature of Patient: _____ Date: _____	
Signature of Legal Guardian/representative (if applicable): _____ Date: _____	
Relationship to Patient: _____	
FOR HEALTHCARE ORGANIZATION USE ONLY:	
Amendment has been: Approved Denied	
Signature of Facility Privacy Officer (FPO): _____ Date: _____	
<input type="checkbox"/> Patient has not filed a Statement of Disagreement, but requests that any future releases include the requested amendment and denial information.	
<input type="checkbox"/> Patient has filed a Statement of Disagreement that must be released along with other documentation with any future releases of information.	
<input type="checkbox"/> Facility/provider appended written response (rebuttal) and forwarded to patient.	
<input type="checkbox"/> Facility/provider did not provide a response/rebuttal	

Reference: Policy PHI.003, Patients' Right to Amend
Revised 2/2018

- Right to request an amendment of information within the DRS
- Request must be in writing
- Facility may deny the requested amendment
- Patient will be notified via letter from the FPO

Accounting of Disclosure (AOD)

Includes all releases of the DRS except those:

- Authorized by the patient
- Used for law enforcement agencies that have custody of an inmate
- Used for treatment, payment or health care operations
- Disclosed as part of a limited data set
- Released to individuals themselves
- Releases that occurred before April 14, 2003
- Used for national security or intelligence purposes

Additional requirements forthcoming as a result of HITECH regulations



Right to Privacy Restrictions

- Requests for such restrictions must be made in writing to the FPO
- No other facility employee may process such a request unless specifically authorized by the FPO.

For example: “I don’t want my information shared with anyone outside the hospital.” - This would not be appropriate because information is required for state reporting and also for accreditation purposes (e.g. TJC).

Confidential Communications

- Patients can request the use of an alternate address or phone number
- If there is a failure to respond by the patient, then the facility may revert to permanent address or phone number to collect payment
- Request must be communicated with facility FPO to work with the SSC FPO

Patient Privacy Complaints

- Route all patient privacy complaints to the FPO
- A complaint log must be maintained in accordance with the Privacy Complaint Process PHI.022
- Complaints must be investigated and documented with corrective action, if applicable
- There may be no retaliation due to a complaint being made
- Disposition of complaint must be consistent with PHI.023 Sanctions for Privacy and Security Violations policy
- The RL Solutions is the module used for complaint tracking

Safeguarding PHI

- Log off terminals when not in use and NEVER share your password
- Computers should have screen savers whenever possible
- Computer screens should be positioned so PHI is not readable by the public or other unauthorized viewers
- Printers should be positioned in protected locations so that printed information is not accessible or viewable by an unauthorized person
- PHI must be securely disposed of (e.g., shred bins)
- Double-check fax numbers prior to hitting “ Send”

Impacts on Patient Care Areas / Ancillaries

- Passcode for family members and friends
- Patient rights may be requested at any time during hospitalization
- Verification of Requestors
- Required accounting of disclosures
- Photography policy

Examples of Privacy/Security Issues

- Lack of knowledge regarding permitted uses of PHI
- Discussions of patient information in public places such as elevators, hallways and cafeterias
- Printed or electronic information left in public view (e.g., charts left on counters)
- PHI in trashcan
- Not using appropriate safeguards when emailing or faxing
- Records that are accessed without need to know in order to perform job duties

Examples of Privacy/Security Issues Cont.

- Inappropriate control or use of documents containing PHI – paper or electronic
- Sharing PHI without an authorization when one is required
- Sharing passwords
- Failure to act proactively to prevent, detect, or correct privacy or security breaches
- Discussing patient information on social networking sites (e.g., Facebook, Twitter)

Sanctions

- There is a sanctions policy to address privacy and information security violations
- Types of violations can include:
 - Negligent (accidental or inadvertent)
 - Intentional (purposeful)
- For specific information on sanctions policy contact FPO and/or review the facility's policy

For More Information Review:

PHI.023 Sanctions for Privacy & Information Security Violations

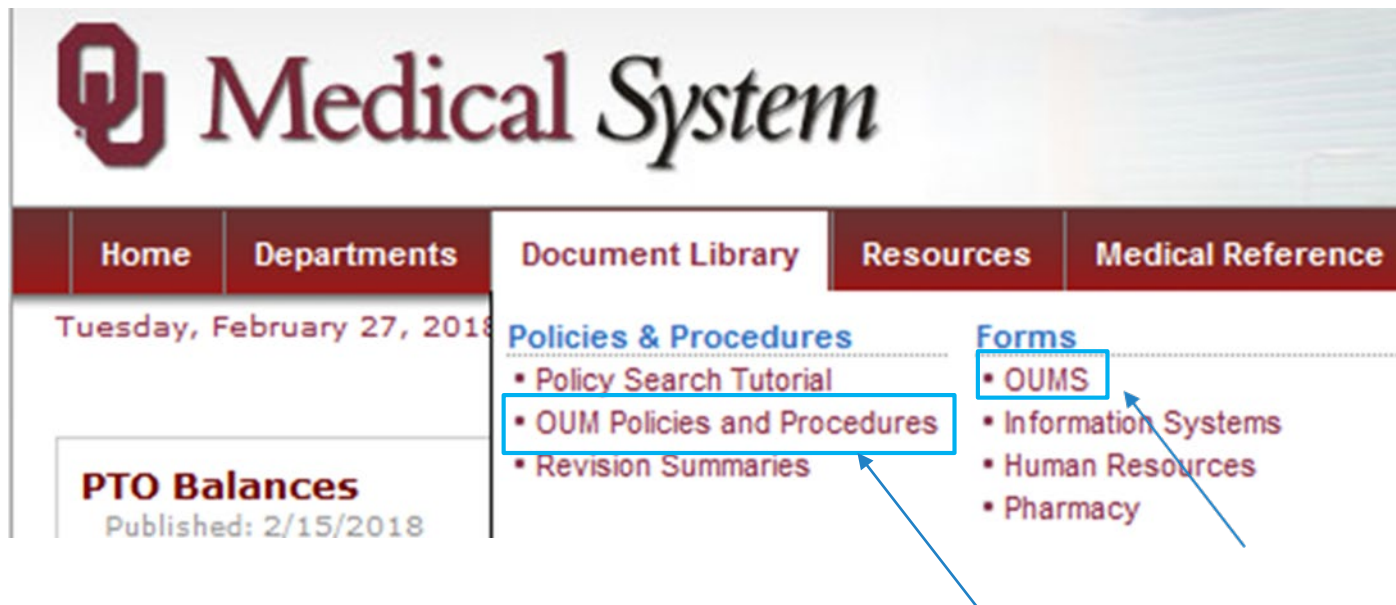


Test Your Knowledge

- Do you know who your FPO is?
- What kinds of privacy rights does the patient have?
- Can a patient amend their record?
- Do you know who to refer patient privacy questions or complaints to?
- What is an Accounting of Disclosures?
- When can you access, use or disclose the patient's PHI?
- Where do you dispose of patient information?



Patient Privacy Policies and Forms on the Intranet



OUM Privacy Policies

- PHI.001 - Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information
- PHI.002 - Protecting and Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Personally-Identifiable Information
- PHI.003 - Patients' Right to Amend
- PHI.004 - Patients' Right to Request Privacy Restrictions
- PHI.005 - Accounting of Disclosures
- PHI.006 - Protected Health Information Breach Risk Assessment and Notification
- PHI.007 - Notice of Privacy Practices
- PHI.008 - Safeguarding Protected Health Information
- PHI.009 - Minimum Necessary
- PHI.010 - Patients' Right to Request Confidential Communications
- PHI.011 - Patient Privacy Program Requirements

OUM Privacy Policies Cont.

- PHI.012 - Privacy Official
- PHI.013 - Fundraising Under the HIPAA Privacy Standards/HITECH
- PHI.014 - Community Clergy Access to Patient Listings under the HIPAA Privacy Standards
- PHI.015 - Designated Record Set
- PHI.016 - Determination of Uses & Disclosures of De-Identified Info
- PHI.017 - Authorization for Uses & Disclosures of PHI
- PHI.018 - Hybrid Entity
- PHI.019 - Limited Data Set & Data Use Agreement
- PHI.020 - Marketing Under the HIPAA Privacy Standards
- PHI.021 - Patient's Right to Opt Out of Being Listed in Facility Directory
- PHI.022 - Privacy Complaint Process

OUM Privacy Policies Cont.

- PHI.023 - Sanctions for Privacy & Info Security Violations
- PHI.024 - Uses & Disclosures for which an Authorization or Opportunity to Agree or Object is not Required
- PHI.025 - Uses & Disclosures of Protected Health Info to Other Covered Entities & Health Care Providers Under the HIPAA Privacy Standards
- PHI.026 - Uses & Disclosures of PHI for Involvement in Patient's Care & Notification Purposes
- PHI.027 - Uses and Disclosures Required by Law
- PHI.028 - Uses Verification of External Requestors
- PHI.029 - Electronic Incident Response
- PHI.030 - Confidential Patient Status
- PHI.031 - Photographing, Video Monitoring,/Recording, Audio Monitoring/Recording, and/or Other Imaging Policy
- PHI.032- Patients' Right to Access

An aerial photograph of a city, likely Denver, showing a mix of residential houses and commercial buildings. A large, semi-transparent red rectangle is overlaid across the center of the image, serving as a background for the text.

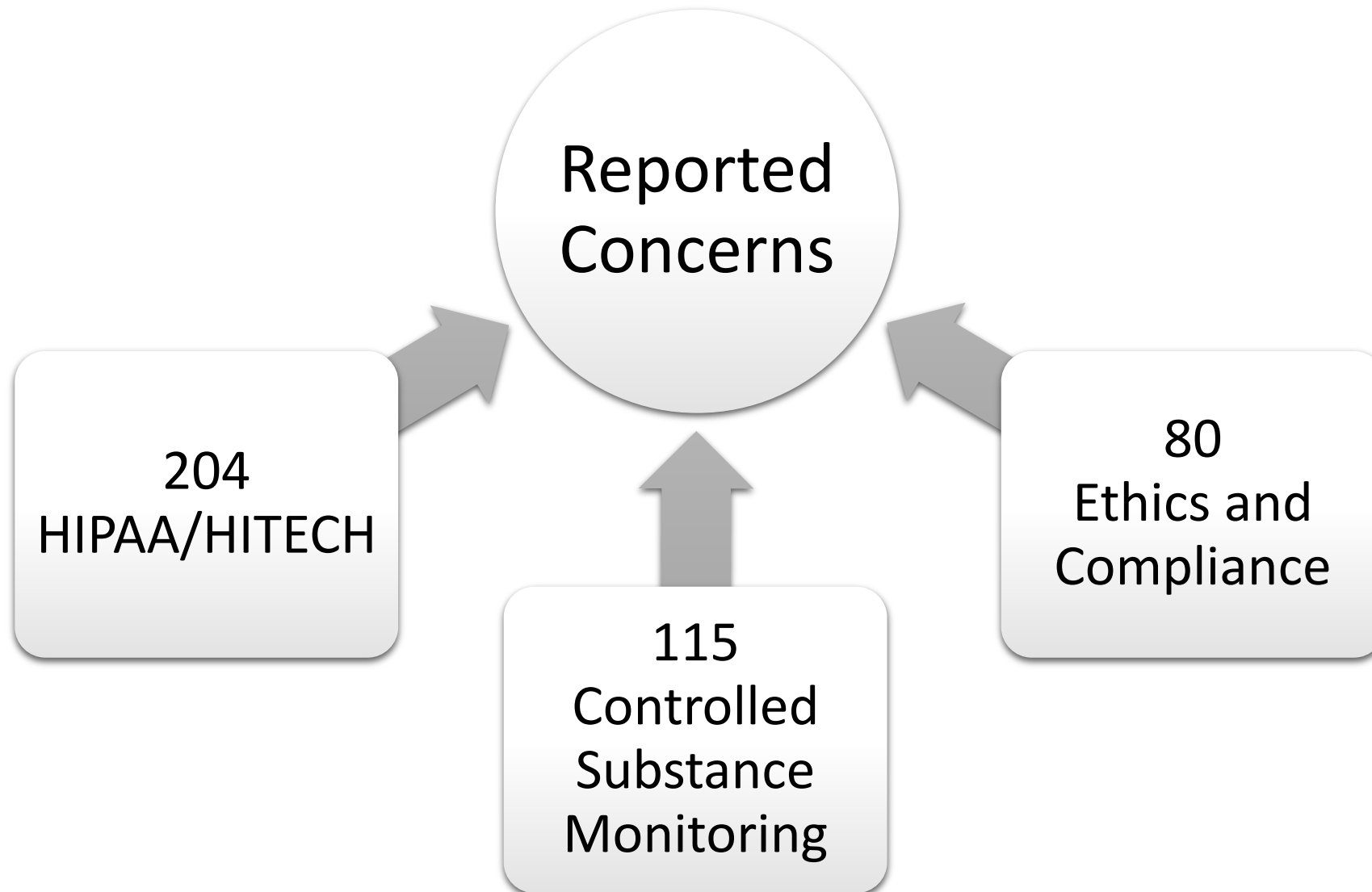
Thank you for your attention and for protecting our patient's PHI.

Every patient, every time!



**2020 Code of Conduct
Refresher Training**

2019 Reported Cases



Ethics and Compliance

Harassment and Bullying

All OUM employees have the right to work in an environment free of harassment and bullying.

An environment free of harassment is one where all individuals are accepted and treated fairly regardless of any diverse characteristics or cultural backgrounds. All OU Medicine colleagues can expect to work in an environment free of harassing conduct to include sexual harassment of any kind.



Harassment and Bullying

Other examples of workplace harassment and bullying include:

- Changing of schedules out of turn
- Unwanted nicknames or labels
- Gossiping or spreading rumors about colleagues (including physicians)
- Pinning staff against one another
- Purposeful exclusion from conversations or withholding of information

Conflict of Interest & Solicitation

A conflict of interest may occur if an OUM colleague's outside activities, personal financial interests, or other private interests interfere or appear to interfere with his/her ability to make objective decisions in the course of the colleague's responsibilities as an OUM employee.

OUM colleagues are obligated to remain free of conflicts of interest in performance of their responsibilities at OU Medicine.

If a conflict of interest should present itself, the OUM colleague must disclose all pertinent information to their leader.

OUM Leaders, Directors and above, are required to complete a Conflict of Interest form annually in compliance with EC.005.

Additionally, OUM colleagues must not solicit referrals or resources to any company with which they have a vested interest. This includes the donation of supplies, monetary contributions or advertisement.

Falsification of Documents

No OU Medicine colleague should alter or falsify information under any circumstances.

OU MEDICAL SYSTEM
Refrigerator/Freezer Log
Location of Refrigerator/Freezer: _____

Month: _____ Unit: _____

Type of Refrigerator/Freezer: ☐ Patient Food ☐ Medication Refrigerator ☐ Other (list) _____

Date	Time AM	Refrigerator Temperature	Freezer Temperature	Signature AM	Time PM for immunizations Only	Refrigerator Temperature	Freezer Temperature	Signature PM	Min/Max if Closed on weekends	Corrective Action (What you did to get the temp into range)
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										

OU MEDICAL CENTER
Automated Dispensing Machine Daily Discrepancy Log
UNIT / LOCATION: _____ COST CENTER: _____ MONTH / YEAR: _____

Day	Discrepancies Exist? (Circle One)	Signatures		Day	Discrepancies Exist? (Circle One)	Signatures	
		Off-going Nurse	On-coming Nurse			Off-going Nurse	On-coming Nurse
1	Y N	/	/	1	Y N	/	/
2	Y N	/	/	2	Y N	/	/
3	Y N	/	/	3	Y N	/	/
4	Y N	/	/	4	Y N	/	/
5	Y N	/	/	5	Y N	/	/
6	Y N	/	/	6	Y N	/	/
7	Y N	/	/	7	Y N	/	/
8	Y N	/	/	8	Y N	/	/
9	Y N	/	/	9	Y N	/	/
10	Y N	/	/	10	Y N	/	/
11	Y N	/	/	11	Y N	/	/
12	Y N	/	/	12	Y N	/	/
13	Y N	/	/	13	Y N	/	/
14	Y N	/	/	14	Y N	/	/
15	Y N	/	/	15	Y N	/	/
16	Y N	/	/	16	Y N	/	/
17	Y N	/	/	17	Y N	/	/
18	Y N	/	/	18	Y N	/	/
19	Y N	/	/	19	Y N	/	/
20	Y N	/	/	20	Y N	/	/
21	Y N	/	/	21	Y N	/	/
22	Y N	/	/	22	Y N	/	/
23	Y N	/	/	23	Y N	/	/
24	Y N	/	/	24	Y N	/	/
25	Y N	/	/	25	Y N	/	/
26	Y N	/	/	26	Y N	/	/
27	Y N	/	/	27	Y N	/	/
28	Y N	/	/	28	Y N	/	/
29	Y N	/	/	29	Y N	/	/
30	Y N	/	/	30	Y N	/	/
31	Y N	/	/	31	Y N	/	/

Weekly Manual Narcotic Count

Week 1 Date: _____	Week 2 Date: _____	Week 3 Date: _____	Week 4 Date: _____	Week 5 Date: _____
RN Signatures	RN Signatures	RN Signatures	RN Signatures	RN Signatures
/	/	/	/	/

Duty to Report and Cooperate

Each individual has a responsibility to report any activity that appears to violate applicable laws, rules, regulations, accreditation standards, standards of medical practice, federal health care conditions of participation, or the OUM Code of Conduct.

You should first raise concerns with your direct supervisor, manager or director. If this is uncomfortable or inappropriate, you may discuss the situation with the Human Resources Business Partner, the ECO or the Ethics and Compliance Department.

There can be no retaliation for reporting in good faith.

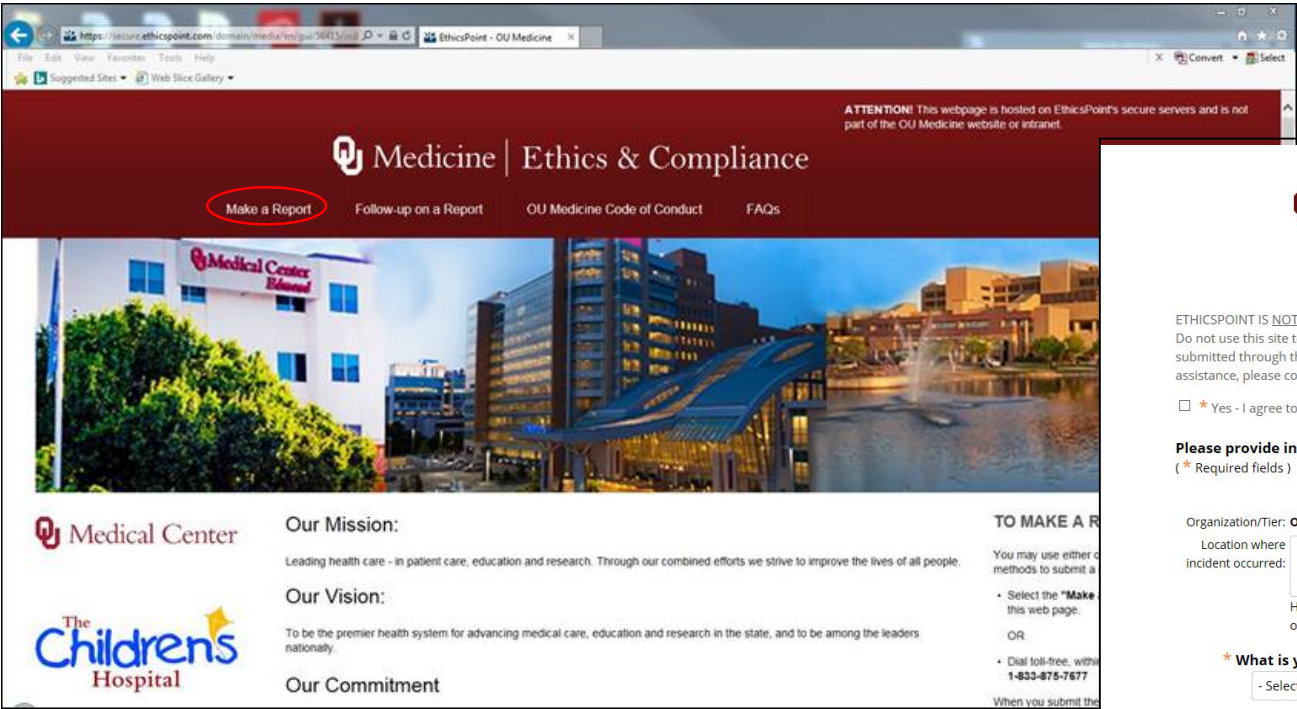
It is required that all OUM colleagues cooperate and participate in any ethics investigation that may take place.



EthicsPoint

You can contact the Ethics Hotline, EthicsPoint, at any time to make a report by calling 1-833-875-7677 or by going to www.oumedicine.ethicspoint.com.

EthicsPoint allows for anonymous reporting by all OU Medicine colleagues.



If you do not wish to remain anonymous, please complete the following:

Your Name: First Name Last Name

Your Phone Number

Your E-mail Address

Best time for communication with you:

Report - Allegation

or file that supports your concern, please upload here:

regarding your concern, to include all individuals involved or /or awareness of the situation and the location. As well as any be valuable in the evaluation and ultimate resolution of this

Please take your time and provide as much detail as possible, but exercise care to not provide details that may reveal your identity unless you wish to do so.

TO MAKE A R

You may use either of the following methods to submit a report:

- Select the "Make a Report" link on this web page.
- OR
- Dial toll-free, within the state of Oklahoma, 1-833-875-7677.

When you submit the report, you will be asked to provide the following information:

Organization/Tier: **OU Medicine**

Location where incident occurred:

Hospital (ie. Building where incident occurred) and Department (ie. Area where incident occurred):

*** What is your relationship to OU Medicine?**

- Select One -

*** Do you wish to remain ANONYMOUS for this report?**

☐ Yes ☐ No



Patient Privacy

Consent

Release of Verbal PHI

- Before discussing PHI in front of family members, visitors or staff, you must obtain consent from the patient to do so.
- When providing new or sensitive information, obtain consent from the patient even if the patient has already consented for PHI to be discussed in front of that individual.
- You must obtain the patient passcode from an individual before releasing patient information if the patient is unable to give consent.

Photo/Video Consent

- Prior to taking photographs or videos of patients or within the hospital, an e-demand photo consent form must be completed.
- Only OUM devices may be used for photography/video purposes.

Patient Verification

Correct Documents-Correct Patient

- Before applying ID bands and/or patient stickers, use two patient identifiers to ensure that the correct identification is being applied to the correct patient and patient chart.

Patient Paperwork

- Prior to discussing and ultimately handing over discharge paperwork to a patient, verify that every page, including prescriptions are meant for the patient at hand.



Safeguarding PHI

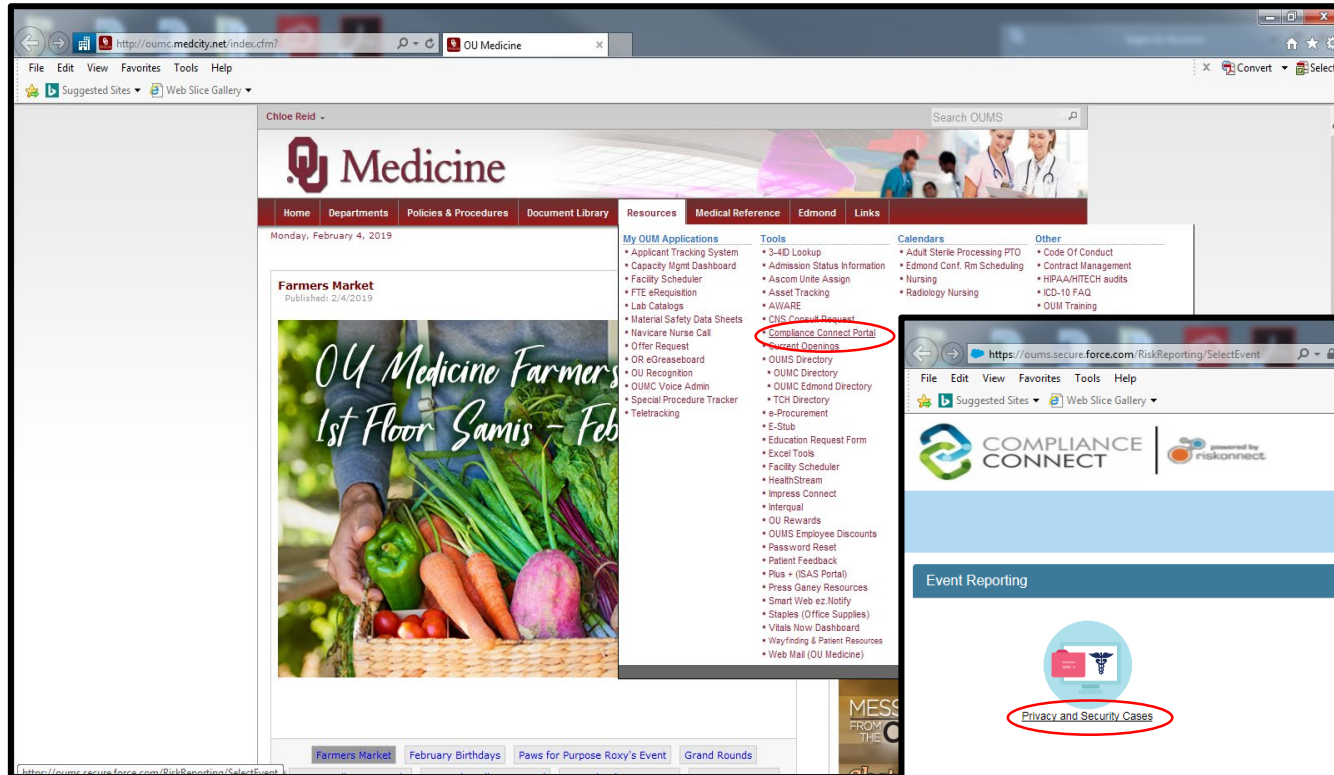
Avoid these common exposures:

- Discussions of patient information in public places
- Printed or electronic information left in public view
- Radiology films in public areas
- Discussing patient information on social networking sites
- PHI in regular trash or sharps bins
- White boards or monitors with full patient name

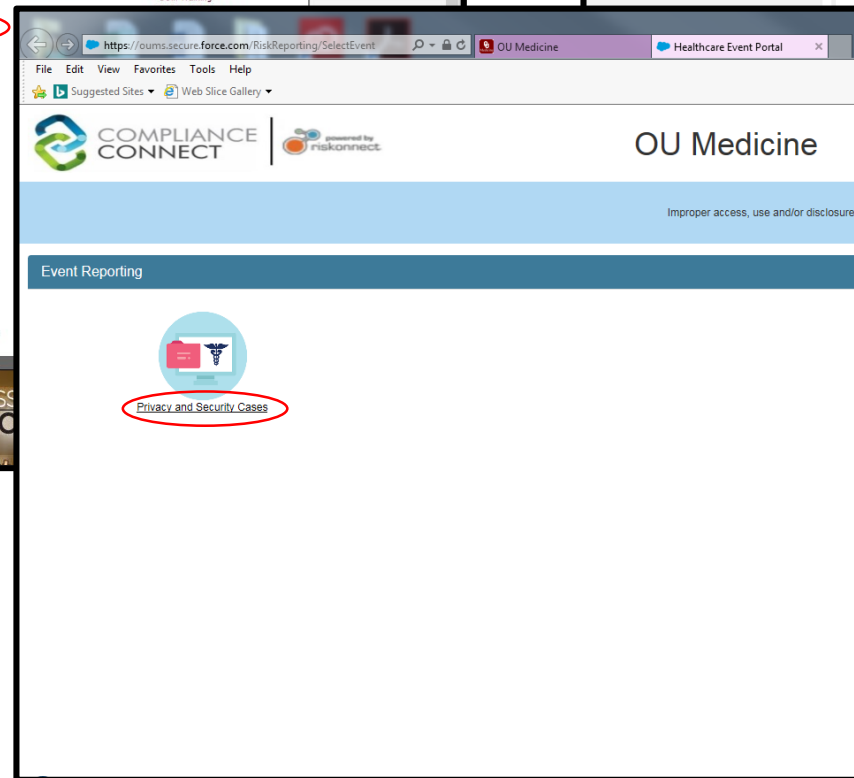


Compliance Connect

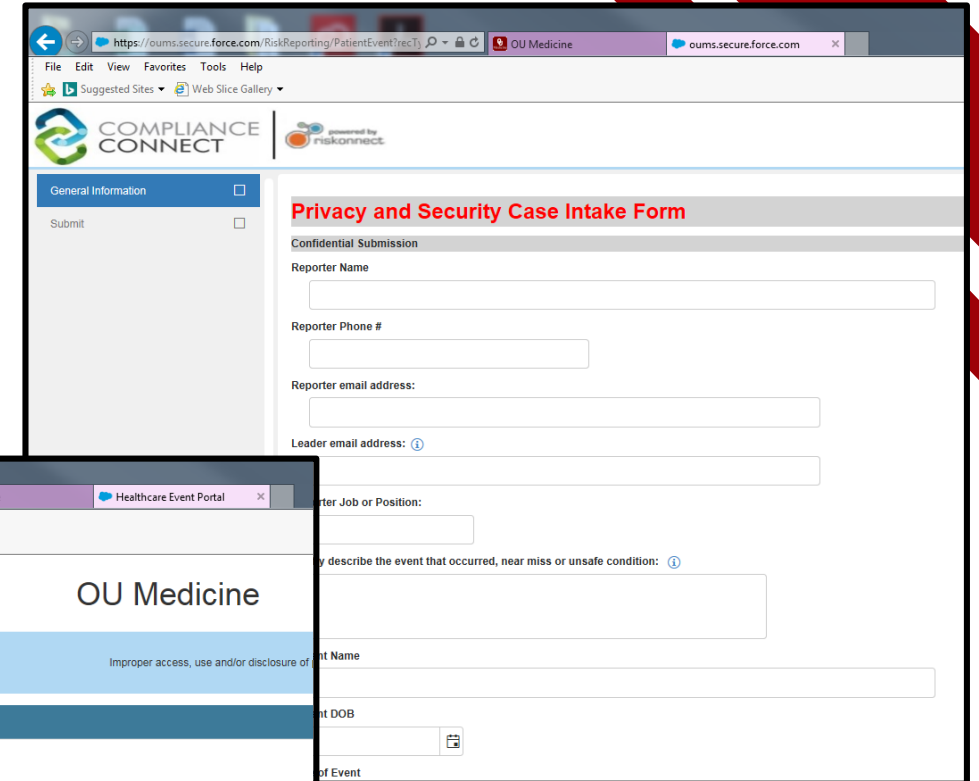
Reporting HIPAA/HITECH Breaches



This screenshot shows the OU Medicine website. In the left sidebar, under the 'Resources' section, the 'Compliance Connect Portal' is highlighted with a red circle. The website header includes the OU Medicine logo and navigation tabs for Home, Departments, Policies & Procedures, Document Library, Resources, Medical Reference, Edmond, and Links. The main content area features a 'Farmers Market' announcement and a search bar.



This screenshot shows the Compliance Connect portal. The 'Event Reporting' section is visible, and the 'Privacy and Security Cases' link is highlighted with a red circle. The portal header includes the Compliance Connect logo and the OU Medicine logo. The main content area is titled 'Event Reporting' and contains a link to 'Privacy and Security Cases'.



This screenshot shows the 'Privacy and Security Case Intake Form'. The form includes fields for Reporter Name, Reporter Phone #, Reporter email address, and Leader email address. It also has a section for 'Confidential Submission' and a 'Submit' button. The form is titled 'Privacy and Security Case Intake Form' and is part of the Compliance Connect portal.

Information Security

Information Security

Email Communication

- Prior to sending any sensitive information,
 - Verify that the email recipients are correct
 - Use encryption in the subject line of email if necessary and never place sensitive information in the subject line
 - Do not send sensitive information to an individual's personal email account
- This ensures that you are communicating to the correct individual on a secure network.

User Behavior

- Only access records when necessary for your job
- Never look at the records of your family members, friends, neighbors, etc.

Information Security

Mobile Devices

- Devices must be encrypted
- PHI should never be sent to mobile devices – including pagers and text messages
- Enable passcode protection
- Do not connect devices to unsecured Wi-Fi
- Use discretion when downloading applications
- Avoid storing sensitive information on mobile devices
- Be cautious about internet usage
- Text message/Voicemail phishing



Phishing Scams



What to look for:

- Some of these emails contain characteristics such as:
 - Subject line containing: “Scan Data”, “Scanned Document”, “Your booking #####”, “Documents”
- Abnormal senders
 - info@somecompany.com, Jean-123@somecompany.com, no-reply@mycompany.com

What to do at work:

- Refrain from checking non-OUM email
- Take extra precaution with EXTERNAL emails
- Click the *Report Phishing* button immediately if you have received one of these emails

Controlled Substance Monitoring

Controlled Substances

Prescription and controlled medications and supplies must be handled properly and only by authorized individuals to minimize risks to us and to patients. If one becomes aware of inadequate security of drugs or controlled substances or the diversion/theft of drugs from the organization, the incident must be reported to the supervisor, manager, or director immediately.



Controlled Substances and Medication Diversion Team

OU Medicine employs a robust diversion prevention and surveillance program that is overseen by the Medication Diversion Team. The necessity of diversion prevention processes is mandated by the Oklahoma Board of Pharmacy Law Title 535: 15-3-2.

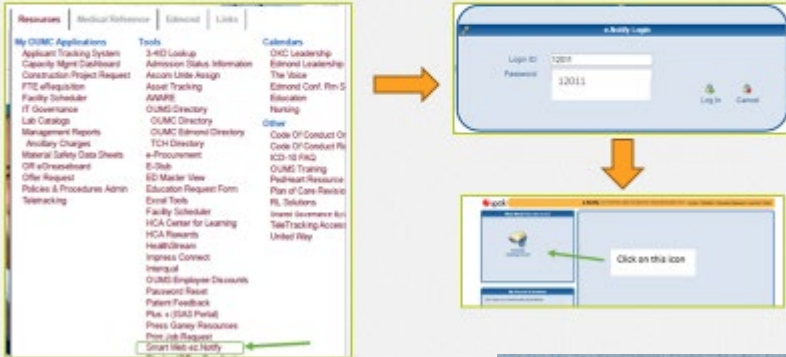
OU Medicine facilities strictly enforce reporting of any violations of diverting medications by facility staff or privileged practitioners in accordance with OUM Policy PHARM.017: DEA and State Controlled Substance Diversion and Loss Reporting.

When and How to Notify the Med Diversion Team (MDT):

The team must be notified immediately of a suspected diversion or diversion currently taking place; if there is suspicious behavior; if the suspect is potentially under the influence of substances that could impair their performance or judgment; and for unaccounted for controlled substances. The MDT must confer and determine appropriate action within 24 hours.

MDT Notification

Announcing a new process



Notifying MDT

Notification of the MDT will be available to all staff on the Intranet via Tools > Smart Web ezNotify > login ID 12011 (password 12011). One would choose to Activate an Existing Event and then choose whether to notify the Edmond Team or the OKC Team.

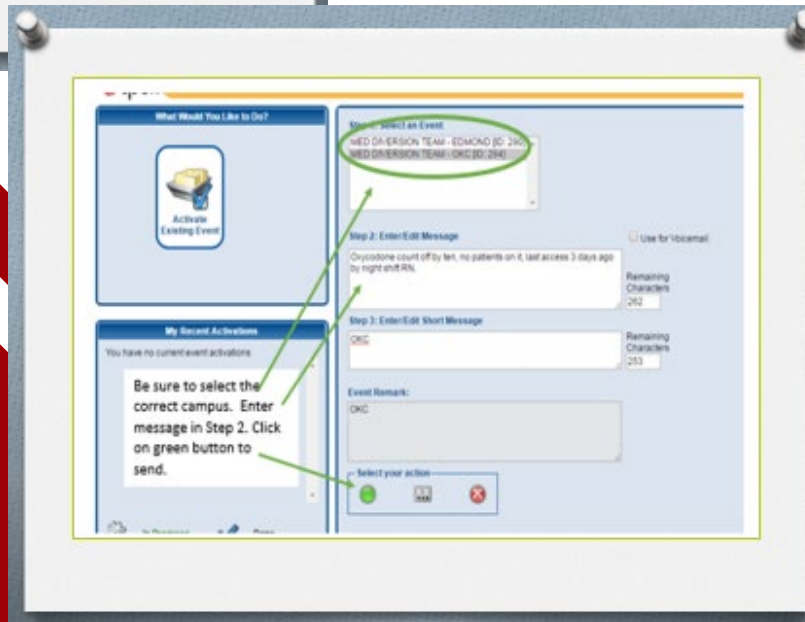
Examples of information to include in the message:

Possible diversion – TCH PICU – contact is Charge nurse Nancy @ 271-2222

Suspicious behavior – OUMC ER – contact is Supervisor Charlie @ 271-7777 – CC notified and UDS in process

Suspect possibly under the influence – Edmond ALC – contact is night coordinator at 359-9999 – UDS in process

PCA discrepancy in the TICU – approximately 20 ml unaccounted for – contact is Charge RN Grace @ 271-1111



Diversion Opportunities

Wasting Controlled Substances

Unused portions of controlled substances, including used fentanyl patches, must be **placed in a CsRX Container** to ensure the medication is not retrievable. Wastes of controlled substances may not be placed in sharps containers, other buckets/bins or trash cans.



Perforated Medication Packs

Medication packs that are packaged by OU Medicine should be divided at the perforation line with scissors to prevent accidental tearing of the pack at the seal. Accidental tearing could result in loss of the controlled substance or an opportunistic moment for someone diverting.



Diversion Opportunities



Physical Items That Are Considered Controlled Substances

Physical items granting access to controlled substances including: keys, prescription pads, prescription paper, printers used for electronically printing prescriptions, etc. are to be treated with the same security and handling measures as controlled substance medications. Theft or loss of any of these items should be reported immediately to your Manager, Director and Med Diversion Team.

Early Signs of Diversion

- Frequent disappearances, in the bathroom or dirty utility room for prolonged periods
- Volunteer for overtime, come to work when not scheduled or often starting a shift early or staying after shift
- Recurrent removal of controlled medications near or at the end of shift or at the end of a stretch of shifts
- Help colleagues medicate their patients and review medication orders of patient they are not caring for
- Heavy or no wasting of drugs
- Picking the same people to waste with
- Pattern of holding waste until oncoming shift



Later Signs of Diversion

- Unpredictable work performance, recurrent mistakes, poor judgement and bad decisions
- Interpersonal relations suffer, become volatile, isolated, sullen
- Blames environment and others for errors
- Tardiness, unscheduled absences, excessive number of sick days used
- Frequent personal crises



Patient Safety

Communication

- Open lines of communication
- Closed-Loop communication
- Questions to reflect on:
 - Do you participate in open communication?
 - Do you promote an environment of understanding where staff and peers are free to ask questions and understand the reasoning behind why certain decisions are made?
 - Are you respectful and receptive of information shared by others and their opinions?
 - Are you intentional when listening to others?



Situation

- ## Background

- ## Assessment

- ## Recommendation

- 
- University of Colorado
Medicine

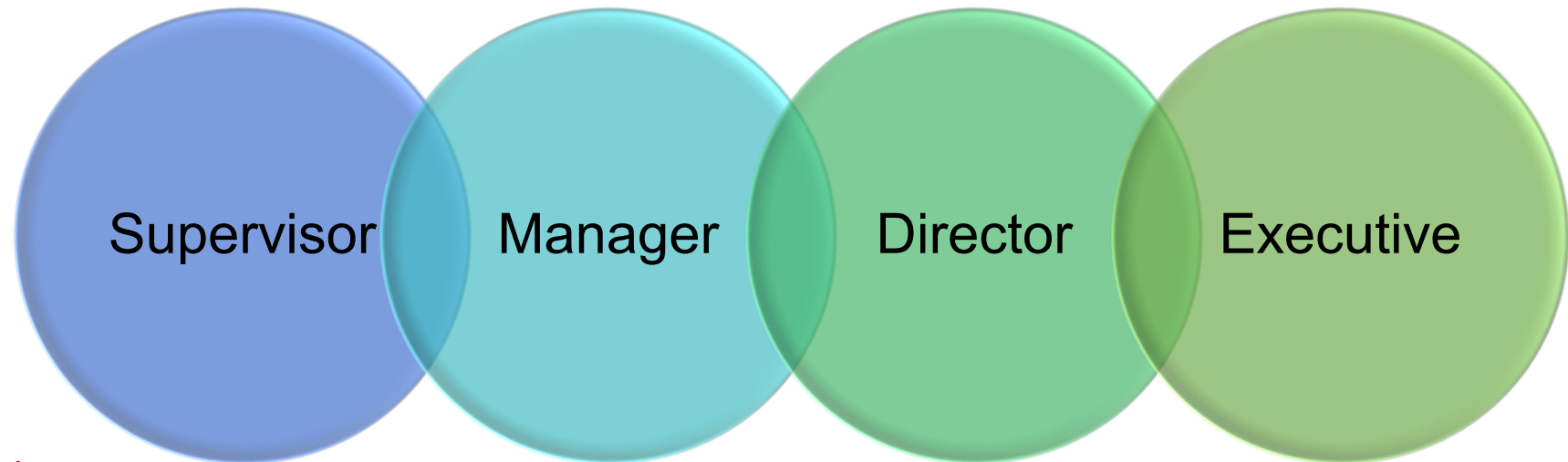
Utilizing Chain of Command

The chain of command includes all levels of leadership.

It is paramount that all OU Medicine colleagues who are confronted with information that they are unfamiliar with or that could potentially put the organization at risk escalate that information through their chain of command rather than attempting to handle it alone.

Additional resources outside your direct chain of command include:

- Clinical Coordinators
- Administrator On-Call



Accountability

It is the responsibility of **all** OU Medicine employees to seek out the necessary information in order to perform their jobs safely and correctly.

After attesting to system policies, departmental processes or other organizational requirements, all colleagues will be held accountable for their ability to speak to and abide by the information.

Examples of information to aid in staying informed include:

Updated
Policy
Changes

Changes to
Departmental
Processes

Regulatory
Requirements

Thank you for completing the



**2020 Code of Conduct
Refresher Training**