



University Partner Training

Version

UP.01

Infant SecurityPage 2

HIPAA/HITECH.....Page 39



Infant Security


OU Medicine

Policy Review

In addition to completing this Healthstream module you will also need to review the following policies:

- OU Medicine Policy: Infant Security
- OU Medicine Policy: Infant/Pediatric Abduction



 OU Medical Center The Children's Hospital OU Medical Center Edmond Breast Health Network	POLICIES AND PROCEDURES PAGE 1 OF 9
TITLE: INFANT SECURITY	POLICY #: SS.002
REPLACES: 15-56	EFFECTIVE DATE: 12/2009, 5/2010, 12/2012, 1/2016, 2/2018

I. **PURPOSE:** To promote the security of newborns.

II. DEFINITIONS:

Perinatal Units: Labor and Delivery, OB Special Care, Mom Baby and Baby Care Area, My Birth Center

Neonatal Units: NICU East, West, North, and South

***Parent:** Biological mother and father of the infant. Father as indicated on the birth certificate or identified by the mother.

Guardian: Person(s) with court appointed custody of the infant.

Guest: Person(s) over the age of 18 identified on the Guest Form by the parent(s).

Visitor: Person(s) over the age of 16 accompanied by a parent.

Sibling: Brother(s) or sister(s) of the infant under the age of 16. Must present an up to date immunization record (upon entrance to the Neonatal Units).

*Adoptive parents are considered guests (if named on the guest list) or visitors (accompanied by the mother or the custodial agency) until court ordered guardianship is obtained.

III. **POLICY:** To promote the security of newborns within inpatient Perinatal and Neonatal services. Infant abduction deterrence is a campus wide approach. Physical security, written protocols, policies, and procedures, as well as staff education and training are to be seamlessly interfaced with campus, facility, and unit security as well as the local community law enforcement to provide total security integration.

IV. PROCEDURE:

Gap Assessment

Annually or when significant changes occur to Perinatal and Neonatal units, all hospitals must complete a self-assessment provided by the National Center for Missing and Exploited Children^{2, 3} and develop a gap analysis (current to compliant state) with an action plan based on findings. (This assessment activity will also support compliance with The Joint Commission Standard EC. 02.01.01 for hospital identification and management of its security risks.)⁴

Hospital and Unit Security Procedures

1. Training for all hospital employees is completed within the first seven days of hire. Additional training for employees involved in the care of newborns is completed prior to or during the employee's first shift in the patient care area.
2. Access to Perinatal and Neonatal care units is limited.
 - a. Proximity locks with badge or card swipe access is recommended.
 - b. Staff that resign from the unit will have their access revoked immediately after their last shift and key pad access codes are changed.

TITLE: INFANT SECURITY

- c. Access codes to units where neonates and/or infants are located are changed at irregular intervals and at a least annually.
 - d. Perinatal and Neonatal unit access doors have “door ajar” alarms.
 - e. Educate staff regarding tailgating/piggy-backing onto secured units.
3. Perinatal and Neonatal Unit ID Badges
- a. All hospital staff, including administrative and ancillary staff, presenting on the Perinatal and Neonatal unit(s), must wear a hospital- issued photo ID badge.
 - b. Perinatal and Neonatal unit staff providing patient care which may involve transporting infants (including agency and traveling nurses) will have a distinctive, hospital-issued Perinatal and Neonatal unit badge to identify them as a member of that unit and having the authority to transport neonates and/or infants.
 - c. Perinatal and Neonatal Medical Staff and Advanced Practice Clinicians providing patient care will have a distinctive, hospital-issued ID badge.
 - d. Ancillary and support staff to Perinatal/Neonatal units will be expected to wear a hospital-issued ID badge and are required to notify unit staff of purpose for presence on the unit.
 - e. Students and Contracted Staff (i.e., audiology services, photography services, etc.) providing additional healthcare services will be expected to wear accompanying school/company ID badge and provided a temporary unit-issued badge with **agreeing facility logo** indicating unit access permission per hospital policy.
 - f. Non-healthcare service providers (i.e., vendors, consultants, construction workers, etc.) will be expected to wear accompanying company ID badge and provided a temporary hospital-issued badge with **agreeing facility logo** indicating hospital access permission per hospital policy.
 - g. All ID badges are worn visibly on the chest area to ensure picture, name, and facility logo are facing outward and unobstructed by pins, decals, or other devices (i.e., double sided badges or a stationary badge may be used).
 - h. ID Badge compliance will be strictly enforced.
4. Perinatal and Neonatal ID Badge Control and Inventory
- a. There will be a control and inventory process for issuance, tracking, and subsequent retrieval of hospital-issued, unit-issued, permanent and/or temporary distinctive ID badges, patches, etc. for Perinatal and Neonatal units.
 - b. Perinatal and Neonatal distinctive ID badges, patches, etc. will be turned in upon termination, resignation or, when the individual is no longer associated with the facility.
 - c. Temporary-issued ID badges issued to students, contractors, etc. are returned to a designated individual on the Perinatal/Neonatal Unit at the end of shift, contracted work hours, etc.
5. Perinatal and Neonatal Unit-Specific Uniforms
- a. Perinatal and Neonatal unit staff should be required to wear unit or hospital-specific attire limited to current employees.
 - b. Attire is unique to perinatal/neonatal unit or hospital by magnet, patches, embroidery, stamps, or watermark which are easy to identify by staff and patients.
 - c. There will be a control and inventory process for issuance, tracking, and subsequent retrieval of hospital-issued, unit-issued permanent and/or temporary distinctive uniforms, patches, etc. for the Perinatal and Neonatal units.
6. Hospital-owned perinatal specific scrubs that are stored on site are kept in a secured environment, with access limited to unit employees and other essential personnel with processes to manage

TITLE: INFANT SECURITY

inventory. Visitor and vendor scrubs are distinctive and are disposed of or returned at the end of each visit.

7. Newborn identification of well born neonates must include:
 - a. Application of mother-father-baby identification bands (four-part) in the delivery room where newborn condition allows.
 - b. If the facility has an electronic infant security system, **application** of the electronic infant security device in the delivery room must take place, where newborn condition allows.
 - c. If the facility has an electronic infant security system, **activation** of the electronic infant security device takes place at the moment the infant is within the security zone (i.e., at delivery, upon transitioning from OR to Perinatal and Neonatal Unit, etc.), where newborn condition allows.
 - d. If the facility does not have an electronic infant security system, or application and/or activation of the electronic security system device is delayed due to physical plant or system default, the infant will be transported by an authorized staff member wearing the authorized Perinatal and Neonatal distinctive badges and uniform using direct, line-of sight supervision.
 - e. If the facility has an electronic infant security system, and removal and/or deactivation of the electronic security system device is required at time of discharge, the infant will remain supervised while on the unit by authorized staff members wearing the authorized Perinatal and Neonatal distinctive badges and uniform using direct, line-of sight supervision until physically discharged from the hospital. Upon discharge, electronic security devices should be removed immediately prior to exiting the perinatal/neonatal unit.
 - f. Obtaining of newborn foot prints in the delivery room, where newborn condition allows. The newborn foot prints become a part of the medical record.
 - g. Documentation of the initial newborn assessment in the delivery room, followed by a more detailed assessment within two hours of birth.
 - h. Facilities that obtain a photograph or video/digital image of the newborn as part of their security process will obtain image within twenty-four (24) hours of birth, after obtaining parental consent.
 - i. Newborn cord blood specimen and any other blood specimen is placed on hold in the hospital laboratory until the day after the newborn/infant's discharge.
8. Identification of premature or compromised neonates should mirror the processes of the well-born once the baby has been stabilized.
9. Bassinets and cribs on Perinatal and Neonatal units should be placed on the side of mother's bed and away from the doors for added security. The same applies for NICU infants undergoing care-by-parent(s) or rooming-in.
10. Perinatal and Neonatal units should minimize the number of times the newborn or infant is removed from the mother's room or a staff supervised unit (Nursery, NICU, Post-Partum, etc.).
11. Perinatal and Neonatal unit staff should perform random security checks throughout the shift (i.e., checking empty rooms, badges, security of doors, etc.).
12. Empty or unoccupied patient room doors should be left open at all times unless the fire marshal or Authority Having Jurisdiction (AHJ) requires otherwise. If doors are equipped with a self-closing mechanism, their operation must not be impeded with devices such as manual hold open devices, furniture, wedges, etc. Self-closing doors should be equipped with automatic hold open devices that

TITLE: INFANT SECURITY

are of appropriate design and connected to the fire alarm system, which ensures closure upon activation of the fire alarm. In the event of a fire, empty or unoccupied patient room doors should be closed.

13. Vendor access will be restricted and allowed only for necessary patient care and safety. Vendor credentials will be verified, and vendor access will be renewed each day.
14. Upon entrance to Perinatal and Neonatal units, all visitors shall be greeted and validated. Hospitals should restrict and monitor visitor entrance, especially within restricted areas on the Perinatal and Neonatal units, such as ORs, Well-Nurseries and NICUs.
15. External vendors and/or agency representatives who are required to interact with the infant and or parents must be appropriately identified upon arrival to unit, and introduced to parents/primary caregivers by the primary care nurse.
16. The Hospital does not support the placement of birth announcements in the newspaper, and provides information warning parents of the danger, including an explanation of the risks of birth announcements in the form of yard signs or outside decorations, or of placement of birth announcements with complete names and addresses in a newspaper.

Parent Education

1. Parent Education- Parents will be educated on security awareness, identification of hospital personnel, primary care staff for the shift, and communication regarding unit activities and any procedures involving the newborn or infant. Parents/primary caregivers will sign a form acknowledging an understanding of infant security education provided and shared responsibility for maintaining infant security during hospital stay. Documentation will be included in the patient's medical record (Attachment A). Language and cultural barriers may interfere with the understanding of, or compliance with, infant security education. Therefore, efforts should be made to achieve optimal understanding by the parent and documented in the medical record.
2. Perinatal Units should have a process for visitor check-in (i.e. visitor log book, visitor ID validation, visitors receive a distinctive visitor wrist band, or name tag allowing entry to the unit, etc.). The wrist band will be a cut away, non- transferable disposable band.
3. Based upon home-care needs of the infant at the time of discharge, parents/primary caregivers will be educated regarding in-home care vendors and other out-patient clinical services. Home Care education will include:
 - a. Vendor/agency name
 - b. Purpose of visit
 - c. Anticipated arrival
 - d. Expected vendor/agency representative identification
 - e. Advisory to parents to remain present with the infant in the home during the vendor/agency representative's visit.

Infant Abduction-Drills, Potential and Actual

TITLE: INFANT SECURITY

1. Infant abduction drills will involve the entire campus and will be conducted at a minimum of once per quarter. The drills will involve each shift, as well as during shift change. The goal is to provide each employee an opportunity to participate in a drill on an annual basis.
2. Hospital staff should be alert to any unusual behavior they encounter from individuals. The alert process should include the recommendations provided by the National Center for Missing and Exploited Children¹ and generate a communication and action plan based on observation and findings.
3. To assist in the timely identification of an abducted infant and/or an abductor, the hospital response for infant abduction includes :
 - a. activating a designated code referencing the abduction of a newborn or infant
 - b. performing a hospital-wide overhead page notification, which should include the unit from which the infant was abducted, gender and age of the infant, and a description of abductor, if available
 - c. having a designated representative responsible for communicating with Law Enforcement agencies, relaying and updating information, as well as receives communication from Law Enforcement for further instructions.

Technology

OUM maintains a list of preferred vendors and negotiated agreements that meet the following requirements. If the facility chooses to purchase a non-preferred product, or initiate its own agreement, then the security product and agreement must meet the minimum requirements listed below.

1. High volume/high traffic units with multiple exits or blind areas should have an electronic infant security system. Appropriate staff should receive formal system training during orientation. The system should be linked to the hospital security team.
2. For Perinatal and Neonatal units, the device must be attached to the newborn and activated in the delivery room as clinically acceptable.
3. Security system must support a device that can only be removed by cutting the band or requires a special removal apparatus, or use skin sensor technology.
4. Infant security band should be adjustable to accommodate weight loss of newborn.
5. Any adjustments to or replacement of security devices required to accommodate weight loss/gain, care requirements, etc. should be done in the presence of the mother or primary caregiver, as clinically acceptable.
6. Security system must integrate with electromagnetic locks, elevators and paging systems, video close-caption cameras, and hospital security.
7. Security system should have the capability to identify infant or child by name, mother/primary caregiver, assigned room and device/tag I.D. number, as well as log date and time of events, archive activities, and create reports.
8. Receiving antenna should not be affected by antenna orientation.

TITLE: INFANT SECURITY

9. Battery backup system in event of power outage.
10. System should have the capability of self-supervision and the ability to visually identify any problems with the system through trouble alarms. Computers supporting running the system should have the "mute" function disabled from the desktop and keyboard. Audible alarms should be located throughout the unit, and not rely on only the computer speakers.
11. One year active transmitter; must be waterproof; expiration date permanently engraved; pulse rate at least 1 time every 10-16 seconds and minimally affected by the application of aluminum to interrupt transmission of security signals.
12. Computer interface with programmable entry codes. Staff that resign from the unit should have their access code revoked immediately after their last shift.
13. Anti-tailgate feature with auto re-arm capability when door closes.
14. Delayed egress capability; continuous door status; perimeter alarm and elevator lockout capability.
15. Security system must be installed and maintained by manufacturer or their representative.
16. Service agreements should support maintenance and updates.
17. Company should have track record of strong customer support.
18. Contracts with the supplier shall require the supplier and the manufacturer to have general liability insurance for bodily injury, death and property loss and damage (including coverage for product liability, completed operations, contractual liability and personal injury liability) in amounts of \$5 million per occurrence and \$10 million in the aggregate with OUM listed as an additional insured.
19. At least quarterly, technology must be evaluated for propensity of false alarms and dead spaces. The evaluations should occur through a collaborative effort involving facility plant operations, security, information technology, nursing management and security system vendor.
20. In the event electronic security systems (i.e., badge access, electronic infant tags, remote door releases, etc.) experience downtime or temporary malfunction, application of physical controls and safeguards (i.e., Security Officer placed at the entrance of the perinatal/neonatal unit) should be implemented immediately.

ATTACHMENTS:

Attachment A: Parent Infant Security Competency Validation

Attachment B: Infant Security Downtime Procedures

REFERENCES:

TITLE: INFANT SECURITY

1. National Center for Missing and Exploited Children (2014). For Healthcare Professionals: *Guidelines on Prevention of and Response to Infant Abductions*, 10th ed. @ http://www.missingkids.com/en_US/publications/NC05.pdf
2. National Center for Missing and Exploited Children (2009). For Healthcare Professionals: *Guidelines on Prevention of and Response to Infant Abductions*, 9th ed. @ www.missingkids.com/InfantAbduction
3. National Center for Missing and Exploited Children (2009). *Self Assessment for Healthcare Facilities* @ http://www.missingkids.com/en_US/publications/NC05assessment.pdf
4. The Joint Commission (January 1, 2012). Comprehensive Manual for Hospitals (CAMH). EC.02.01.01

APPROVED BY:

OUM Policy & Procedure Committee: 1/22/2016

OUM Board of Directors: 1/23/2018

ATTACHMENT A
Parent Infant Security Competency Validation

Patient instructions given (Check appropriate data)	Explained to:		Understands:		Comments:
	Patient Family		Patient Family		
Only give your baby to hospital staff wearing a hospital photo, unit-specific ID badge clearly showing the hospital logo, the caregiver's name, and any unique identifier showing they are authorized to transport infants.					
Always keep your baby in sight. Never leave your baby unattended, even for a moment. Have family members or friends watch the baby while you shower or use the restroom. If they are not available, please call your nurse to transport your baby to the nursery.					
Infants are always transported by bassinet.					
Your baby's identification will be checked with yours each time the baby is brought to your room and each time that you pick up the baby from the nursery.					
Know your nurse on each shift.					
Know when tests for your baby are scheduled. Call the nurse's station if someone you don't know wants to take your baby for an unscheduled test. You have the right to ask to accompany the baby for tests.					
Only give information about you or your baby to people who you know well and trust.					
Consider the risk you may be taking when permitting your infant's birth to be publicized, either through newspaper announcements or by using outdoor decorations such as balloons, door wreaths, or lawn ornaments.					
Do not take your baby off of the _____ unit/floor until you are leaving at discharge.					
Report any unfamiliar people who enter your room and ask questions about your baby by pushing the nurse call button or calling the nursery extension _____.					
When your baby is in the room with you, keep the bassinet beside your bed away from the door.					

ATTACHMENT B

Infant Security- Downtime Procedures

Employees

Will notify:

- Department Supervisor, Director, and/or Clinical Coordinator Immediately.
- Increase awareness and surveillance of anyone in question with a large bag, purse, coat, jacket, etc. While questioning an individual use the following phrase: "We are involved in a Code Pink. May I look inside your bag, purse, coat, jacket, etc.?" If they decline search or exhibit suspicious behavior, do not detain, call OUHSC Police Services and be prepared to provide a detailed description.

Facilities Dispatch

Will notify:

- Firetrol
- OUPD
- Safety Director and/or Manager

Other Nurses/Employees

- Increase awareness and surveillance of anyone in question with a large bag, purse, coat, jacket, etc. While questioning an individual use the following phrase: "We are involved in a Code Pink. May I look inside your bag, purse, coat, jacket, etc." If they decline search or exhibit suspicious behavior, do not detain, call OUHSC Police Services and be prepared to provide a detailed description.

Facilities/Maintenance

- Contact and/or Assist Firetrol
- Increase awareness and surveillance of anyone in question with a large bag, purse, coat, jacket, etc. While questioning an individual use the following phrase: "We are involved in a Code Pink. May I look inside your bag, purse, coat, jacket, etc.?" If they decline search or exhibit suspicious behavior, do not detain, call OUHSC Police Services and be prepared to provide a detailed description.

Charge Nurse, Supervisor, and/or Director


Will notify:

- Facilities Dispatch
- Clinical Coordinator, if they have not yet been notified
- Unit Director, if they have not yet been notified

All Staff:

Increase awareness and surveillance of anyone in question with a large bag, purse, coat, jacket, etc. While questioning an individual use the following phrase: "We are involved in a Code Pink. May I look inside your bag, purse, coat, jacket, etc.?" If they decline search or exhibit suspicious behavior, do not detain, call OUHSC Police Services and be prepared to provide a detailed description.

Remember, you must familiarize yourself with OUM Policy SS.006 Infant/Pediatric Abduction.

 <i>OU Medical Center The Children's Hospital OU Medical Center Edmond Breast Health Network</i>	POLICIES AND PROCEDURES PAGE 1 OF 5
TITLE: INFANT/PEDIATRIC ABDUCTION	
REPLACES: 15-08	EFFECTIVE DATE: 4/2001, 4/2002, 5/2007, 2/2009, 5/2010, 8/2012, 9/2016, 2/2018

- I. PURPOSE:** The purpose of this policy is to establish/describe a prevention system that limits the opportunities for an infant/pediatric abduction, increases the probability of recovery in case of abduction, and describes the actions to be taken in the event of an actual abduction. The system includes 1) staff and parent education regarding the safety of their child and prevention of abduction, and 2) a description of a physical environment that limits the possibility of abduction. This policy further defines specific procedures for employees, Campus Police/Security, Communications, and other hospital personnel to follow in the event of a “Code Pink.”
- II. POLICY:** It shall be the policy of OU Medical System (OUM) that any actual or attempted abduction shall be referred to as “Code Pink.”

Quarterly Code Pink drills will be conducted by the OUM Safety Officer/Safety and Security Subcommittee of the Environment of Care Committee. Drills will serve to increase staff risk alertness and probability of recovery in the case of an actual abduction.

The scope of this policy includes all neonates/infants and children who may be at risk for abduction.

Following an actual or attempted abduction, all involved employees will attend a mandatory debriefing.

Prevention of Infant/Pediatric Abduction:

- A. All employees and OU Health Science Center (OUHSC) Police/Security will be oriented on processes to prevent abduction.
- B. In infant and pediatric areas:
 1. All employees will be on the alert of any suspicious behavior and will immediately notify OUHSC Police/Security of concerns.
 2. The policy will be reviewed by all staff.
- C. Education on abduction risk will be provided on admission to parents of hospitalized neonates/infants and pediatric patients. This information provides guidelines on parental participation in safeguarding their child.
 1. Parents will be advised to always identify staff by hospital badge and picture identification. Parents are advised to never relinquish their child to staff or anyone without proper identification.
 2. Parent education will be documented in the patient chart.

Identification of Infants:

- A. All infants will be identified with a hospital armband on admission.
- B. OU Medical System will not publish birth announcements in public newspapers.

Transport of Infants:

- A. Infants will be transported by a parent or properly identified hospital personnel.
- B. Infants will be transported one at a time.

TITLE: INFANT/PEDIATRIC ABDUCTION

- C. Newborns will be transported in a bassinet, isolettes, cribs, or infant warming beds only.
- D. During maternal and newborn transports, the infant will be transported in mother's arms with the mother in a wheelchair or carrier.

Environment:

- A. Nurseries or units occupied by critically ill infants will have access controlled entries.
- B. The Women's and Newborn Services will provide additional security surveillance.
- C. Neonates will not be left unsupervised. Holding nurseries will be attended at all times.

Areas with Infant Abduction Security Systems

- A. Each unit equipped with an infant abduction security system will perform routine equipment checks to include transponders and audible alarms according to unit/service policy.
- B. Facilities/Maintenance will perform semi-annual preventative maintenance of all infant abduction security systems.
- C. When a system or component of a system fails, the following departments will be contacted:

For OUM Downtown Campus:

- 1. OUHSC Police Services at 271-4911.
- 2. Facility Management at 271-4190.
- 3. Downtown Safety Officer at 271-5808.
- 4. Unit personnel of the affected unit until the system is properly functioning.

For OUM – Edmond Campus:

- 1. Edmond Security Dial 0 for the Operator
- 2. Plant Operations at 5527.
- 3. Edmond Safety Officer at 650-4990.
- 4. Unit personnel of the affected unit until the system is properly functioning.

III. PROCEDURE:
Responsible Party:
Action:

Suspected or Actual Abduction:

Any employee

- 1. If a patient is found missing or suspected as abducted, activates the alarm system and/or immediately notifies: OUM Downtown Campus hospital operator at 271-4190 and the OUM Edmond Campus hospital dial 444. Gives the following descriptive information about the child to the operator.
 - a. Age
 - b. Sex
 - c. The location last seen
 - d. Any additional description to help searchers recognize the child...clothing, hair color, etc.
- 2. In the nursing care areas, notifies the Charge Nurse.
- 3. If the description involves an infant or small child, questions anyone with a large bag, purse, coat, jacket, etc. While questioning an individual use the following phrase: *"We are involved in a Code Pink. May I please look into your bag, purse,*

TITLE: INFANT/PEDIATRIC ABDUCTION

coat, jacket, etc.” If they decline this search or exhibit suspicious behavior, do not detain, call the OUHSC Police/Security and be prepared to provide a detailed description.

4. Immediately checks all adjacent stairwells and exits.
5. Immediately reports any suspicious individuals to the OUHSC Police/Security.

Hospital Operator

1. Announces “Code Pink” and provides any descriptions given by the staff (example: “Code Pink. This 4-year-old male child was last seen on the 8th floor of Children’s Hospital. He has blond hair and is wearing crimson OU pajamas”).
NOTE: Due to Health Insurance Portability and Accountability Act (HIPAA) requirements, patient names can never be use for announcements.
2. Transfers the caller to the OUM Downtown Campus Police at 271-4911 and OUM Edmond Campus Security at 5527 during normal hours or 921-6959 after hours.

Other Nurses/Employees

1. Immediately checks all adjacent stairwells and exits for the child and/or suspicious individuals and reports concerns to the OUHSC Police/Security as soon as possible.

OUHSC Police/Security

1. Notifies, not necessarily in this order, the following as deemed appropriate:
 - a. Oklahoma City Police Department/Edmond Police Department.
 - b. Capitol Patrol.
 - c. Facilities/Maintenance at Downtown Campus: 271-4190. Plant Operations at Edmond Campus: 5590
 - d. Federal Bureau of Investigation (FBI) – 290-7770.
 - e. Center for National Missing and Exploited Children – (800) 843-5678.
 - f. Public Relations - 271-7900. Edmond 359-5580
 - g. Risk Manager at Downtown Campus: 271-8050 or through the page operator and 6318 for the Edmond Campus.
2. Assists in the investigation and search.
3. Responds to inquiries of other patients, providing minimal information and alleviating stress of the other patients; respect the confidentiality of the involved.

**OUHSC Police Dispatcher
for OUMC- Downtown**

1. Sends officers to the scene.
2. Notifies the OUHSC Police supervisor on duty.
3. Notifies the OUHSC Police Director.

**Security/OUHSC Police
Director/Shift Supervisor**

1. Conducts a search of the hospital(s), both interior and exterior.
2. Secures exits, including parking facilities.

TITLE: INFANT/PEDIATRIC ABDUCTION

OUHSC Chief, Major or Captain, Edmond Police Department	<ol style="list-style-type: none"> 1. Assumes command of the investigation. 2. Identifies a law enforcement commander
Facilities/Maintenance Director/Employees	<ol style="list-style-type: none"> 1. Stations day shift staff in exterior zones as designated by the Director of Facilities/Maintenance. 2. After hours, on-duty personnel reports to the affected unit to assist.
Supervisor/Charge Nurse or Designee	<ol style="list-style-type: none"> 1. If code Pink is activated notifies: <ol style="list-style-type: none"> a. Unit Director and/or Clinical Manager b. Clinical Coordinator c. Chaplain d. Social Services
Director of Unit Involved	<ol style="list-style-type: none"> 1. Notifies: <ol style="list-style-type: none"> a. Chief Nursing Officer/Associate Chief Nursing Officer b. Administrator On-Call c. Physician of patient.
Physician	<ol style="list-style-type: none"> 1. Informs the parent(s) of the possible abduction.
Nurse Caring for Mother/ Infant/Child	<ol style="list-style-type: none"> 1. Remains with the parents until the Chaplain and/or Social Service staff arrives.
All Staff	<ol style="list-style-type: none"> 1. Continues to search the area. 2. Remains on the unit until released by Nursing Administration and the Police Department.
Chaplain/Social Services	<ol style="list-style-type: none"> 1. Provides comfort and reassurance to the parents. 2. Assists in debriefing staff after incident.
To Cancel a Code Pink if the Child is Found	
Supervisor/Charge Nurse	<ol style="list-style-type: none"> 1. At OUM Downtown: Notifies Police Dispatch at 14911 to cancel the Code Pink. 2. At OUM Downtown: Notifies Communications at 11911 to cancel the Code Pink. 3. At OUM Edmond: notify the Operator by dialing "0" to cancel the Code Pink
To Cancel a Code Pink	
Oklahoma City Police Officer/FBI/Edmond Police Department	<ol style="list-style-type: none"> 1. Instructs the nurse in charge and/or the OUHSC officer and/or the hospital administrator to cancel code pink (as above)

APPROVED BY:



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

POLICIES AND PROCEDURES PAGE 5 OF 5

POLICY #: SS.006

TITLE: INFANT/PEDIATRIC ABDUCTION

Nursing Policy & Procedure Committee: 8/3/2016

OUM Policy & Procedure Committee: 9/22/2016

OUM Board of Directors: 1/23/2018

Objectives

After completion of this module staff should be able to:

- Identify safety measures in place to secure infants within perinatal and neonatal services.
- Demonstrate appropriate safety measures
- “every patient, every time.”
- Recognize individuals exhibiting characteristics of an abductor.



The birth of a baby is a joyous occasion for parents and families. To ensure the joyous event is not disrupted, infant security is of utmost importance at OU Medicine.

Infant abduction deterrence requires a whole system approach including not only training/education for staff, families and visitors, but also includes many facility and equipment measures.

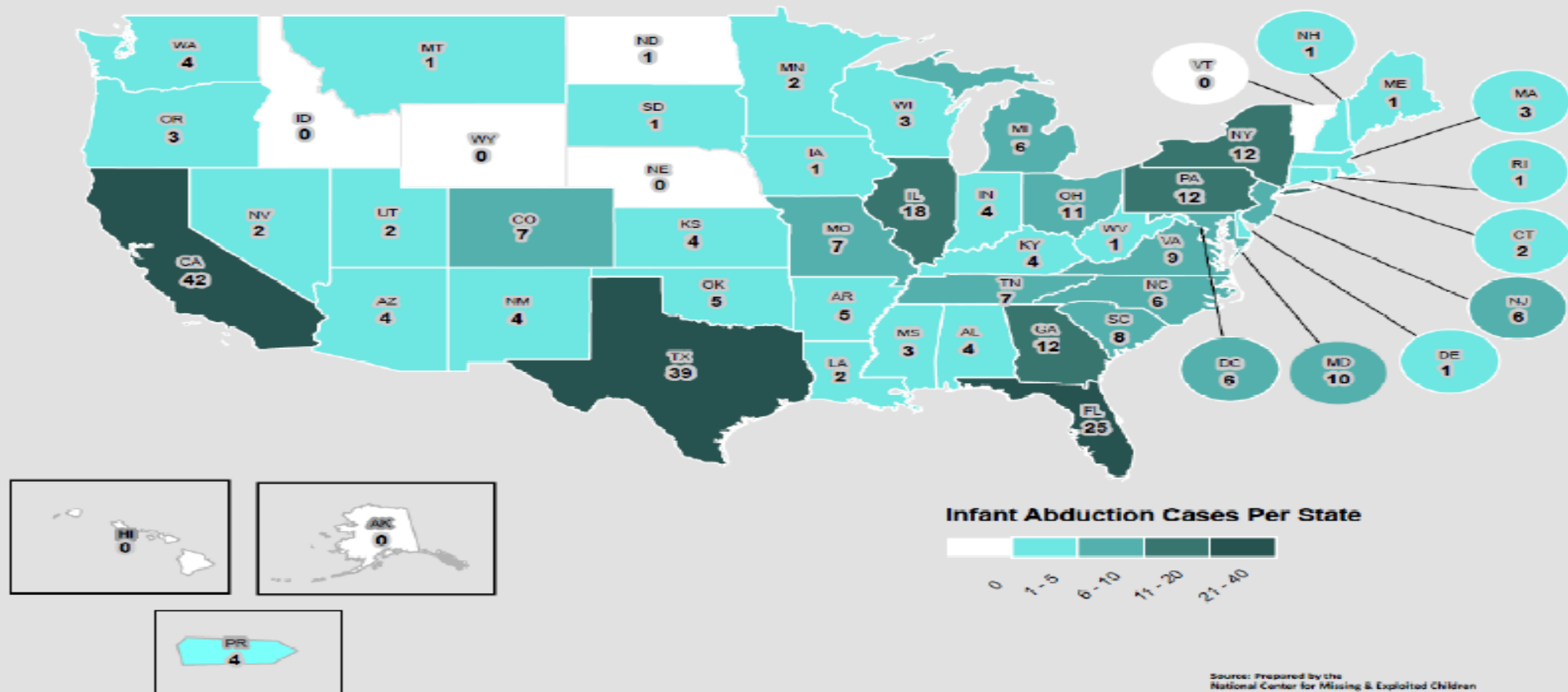


Since 1991, the National Center of Missing & Exploited Children reports there are on average 11 infant abductions each year.

Oklahoma reports 5 infant abduction between 1983-2017



Infant Abduction Cases per State



Sources: Prepared by the
National Center for Missing & Exploited Children
Mapping software donated to NCMEC by Esri, Redlands, California
Updated August 25, 2017

One infant abduction is too many.

An infant abduction is a tragedy for everyone – the infant, parents, staff and medical center.

In order to prevent such an occurrence, security measures must be in place and staff must be ever vigilant.



Definitions

Perinatal Units:

- Labor and Delivery
- OB Special Care
 - Mother/Baby
 - OB ED

Neonatal Units

- NICU East
- NICU West
- NICU North
- NICU South



Definitions

Parent:

Biological mother and father of the infant; father as indicated on the birth certificate or identified by the mother.

Guardian:

Person(s) with court appointed custody of the infant.

Adoptive parents are considered guests (if named on the guest list) or visitors accompanied by the mother or the custodial agency) until court ordered guardianship is obtained.



Definitions

Guest:

Person(s) over the age of 18 identified on the guest form by the parent(s)

Visitor:

Person(s) over the age of 16 not on the guest form (must be accompanied by a parent)

Sibling:

- Brother(s) or sister(s) of the infant under the age of 16



Safety Measures

- Staff education
- Staff identification
- Limited access
- “Code Pink”



Staff Education

- Training for all hospital employees is completed within the first seven days of hire.
- Additional training for employees involved in the care of newborns is completed prior to or during the employees first shift in the patient care area.



Identification of Staff

- All perinatal and neonatal employees must wear the following:
 - Pink hospital-issued photo ID badge
 - Black Scrubs attire to be worn only by Perinatal and Neonatal employees
- Students, contracted staff and non-healthcare service providers will wear accompanying school/company ID badge and a temporary hospital-issued badge



Limited Access

- All hospital staff, including administrative and ancillary staff, presenting on the Perinatal and Neonatal unit(s), must wear a hospital- issued photo ID badge. Visible on the chest area.
- Access to perinatal and neonatal care areas are limited to swipe access for essential personnel.
- All parents/guardians, guests and visitors must check in upon arrival to the unit.
- Do not allow “drafting”, piggybacking”, or “tailgating” (allowing individuals to follow into the unit) of visitors at secured entrances of locked units.



Abductor Profile

According to the National Center for Missing and Exploited Children, the following are common characteristics of abductors:

- Female of “childbearing” age (12-53)
- Overweight
- Compulsive
- Manipulative/Deceptive
- Frequently indicates she has just lost a baby or is incapable of having children
- Often married or cohabitating-the desire to provide the companion with a child is often motivation for the act
- Usually lives in the community where the abduction takes place
- Frequently visits nursery/maternity unit at more than one healthcare facility prior to the abduction



Abductor Profile

- Asks detailed questions about the procedures and the maternity/neonatal floor layout
- Frequently uses a fire-exit stairwell to escape
- May abduct from home setting
- Usually plans the abduction, but does not necessarily target a specific infant
- Frequently seizes any opportunity present
- Frequently impersonates a nurse or other allied healthcare personnel
- Often becomes familiar with healthcare staff members, staff members work routines, and victims parents
- Demonstrates a capability to take “good” care of the baby once the abduction occurs



Abductor Profile

- ✓ There is no guarantee an infant abductor will fit this description.
 - ✓ This is only a profile.
- ✓ An infant abductor can be of **ANY** age, sex, or description. INCLUDING a **hospital employee!**



“Code Pink”

- Any actual or attempted abduction is referred to as “Code Pink”
- All employees should be on alert for suspicious behavior



“Code Pink”

- If a patient is missing or suspected as abducted activate the alarm system and/or immediately notify:
 - OU Medicine Downtown Campus at 1-1911 OR OU Medicine Edmond Campus at 444
- Give a description of the child:
 - Age
 - Sex
 - Last location
 - Any additional description (clothing, hair color, etc.)
- Unit charge nurse



“Code Pink”

- Question anyone with a large bag, purse, coat, jacket, etc.
 - Use the following phrase: “We are involved in a Code Pink. May I please look into your bag, purse, coat, jacket, etc.?”
 - If they decline this search or exhibit suspicious behavior, do not detain them, call the OUHSC Police/OU Medicine Edmond Security and be prepared to provide a detailed description of the person.



“Code Pink”

- Immediately check all adjacent stairwells and exits
- Immediately report any suspicious individuals to the OUHSC Police/OU Medicine Edmond Security
- Continue to search the area
- Remain on the unit until released by nursing Administration or Police/Security



“Code Pink”

- If you hear a Code Pink announced, **not in your unit**:
 - Immediately check all adjacent stairwells and exits for the infant and/or suspicious individuals
 - Report concerns to OUHCS Police/OU Medicine Edmond Security
 - Stay on your unit and remain near stairwells and exits until Code Pink is cleared



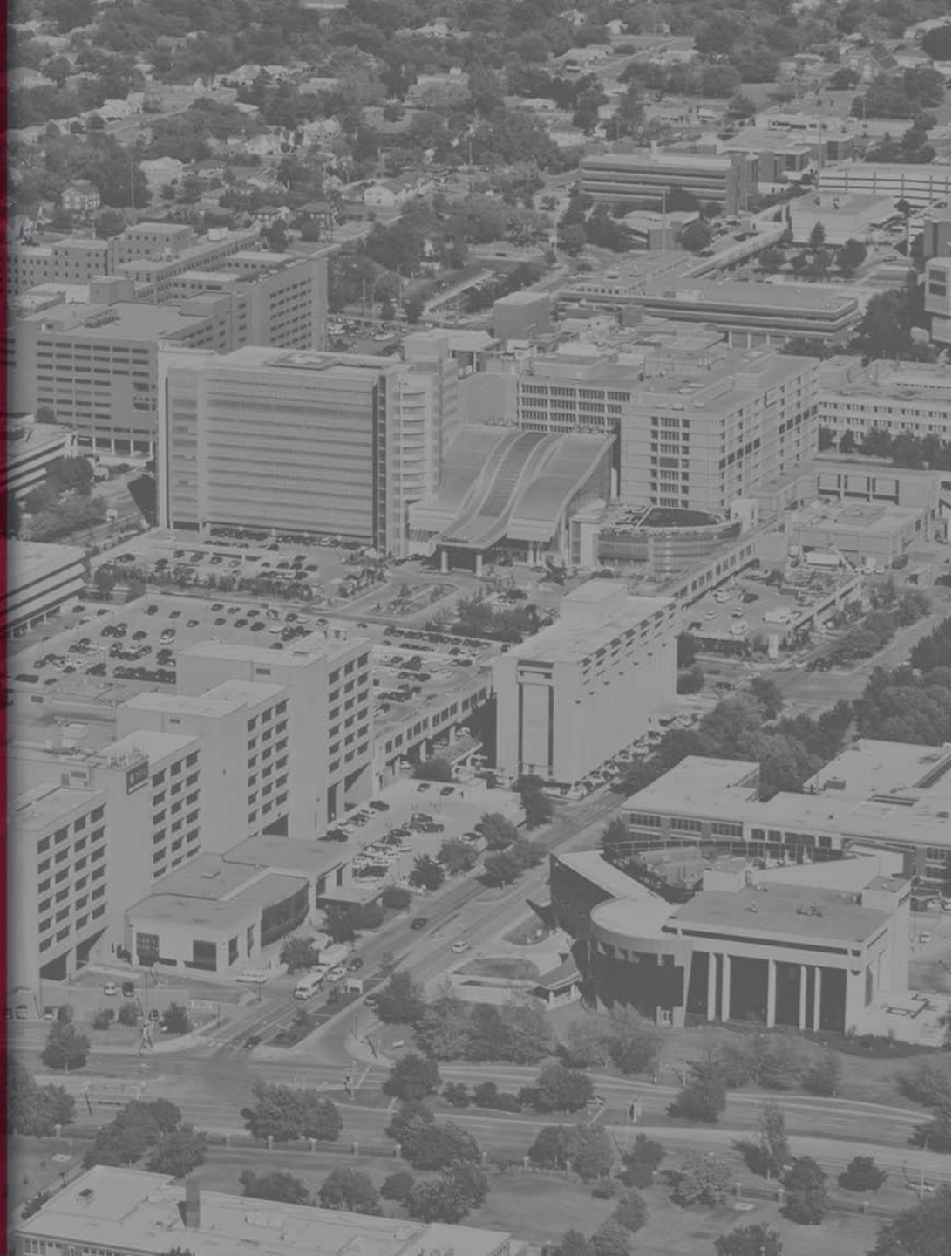




Medicine

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?

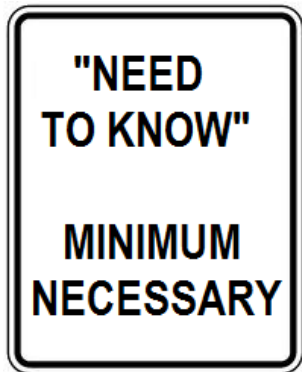
- The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
- Mandatory federal law.

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

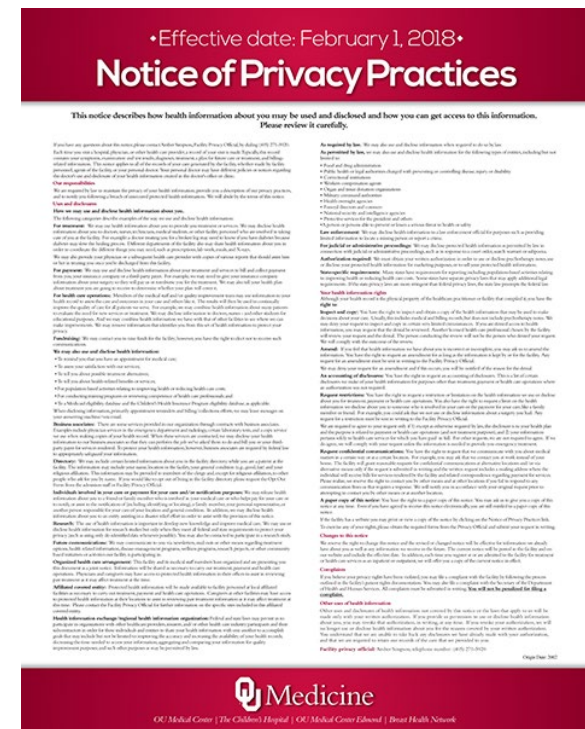
Notice of Privacy Practices

(NOPP)

Given to each patient that has a

- Must be given to each patient that has a face-to-face contact with hospital staff
- Patient must acknowledge receipt of the NOPP
- Must be posted on the website and in each of the registration areas of the facility
- Patient privacy rights are outlined in the NOPP:

Right to Access (Inspect and Copy)
Right to Amend
An Accounting of Disclosures
Right to Request Restrictions
Right to Request Confidential
Communications



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

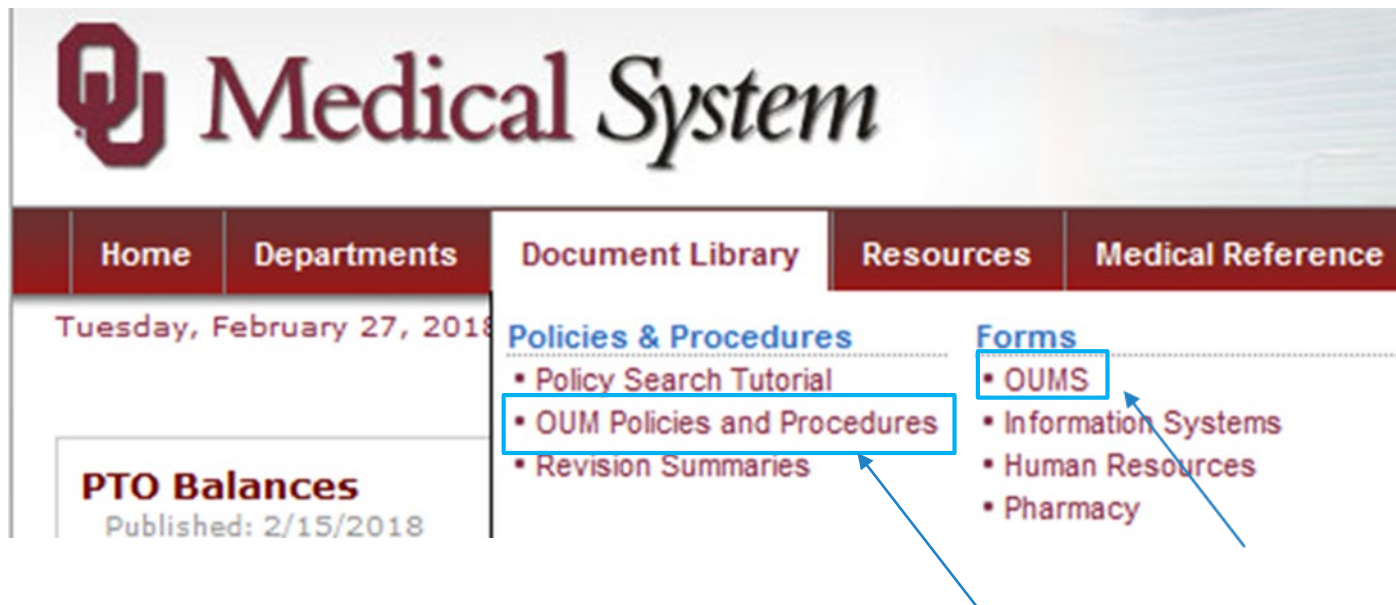


Test Your Knowledge

- 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!