



CARLE FOUNDATION HOSPITAL

May 30, 2008

Dear:

Welcome and we look forward to offering you a challenging and rewarding educational internship/externship at Carle Foundation Hospital.

In an effort to improve service and ensure compliance standards are consistently met, Carle Foundation Hospital has developed a new and centralized process for handling student educational experiences. The new process will go into effect immediately.

Hospital Education will be your point of contact to assess whether all preliminary requirements have been met before you begin your internship. Many of the required elements are necessary to ensure patient safety and privacy as well as your own safety. Tammie Ellingson will be your contact within Hospital Education for all observation only or non-nursing programs. Tammie can be reached by phone at 217-383-4642 or by email at tammie.ellingson@carle.com **You should have the following attached items:**

- Compliance Checklist
- Immunization verification document
- Required immunizations and health standards
- Patient Privacy Agreement
- HIPAA Privacy Rules- You are REQUIRED to read through the rules, sign and return the confidentiality statement indicating that you are aware of the requirements..
- Safety Information- You are responsible for reviewing and retaining this information.

The **Compliance Checklist** indicates what information must be completed before you will be allowed to start your internship. If you have any questions or concerns, please contact Tammie.

Sincerely,

Tammie Ellingson, APN/CNS,CWOCN,CRRN

Manager of the Clinical Education Department

Carle Foundation Hospital

611 W. PARK STREET • URBANA, IL • 61801
PHONE: 217-383-4642 • FAX: 217-383-3121

**CARLE FOUNDATION HOSPITAL & AFFILIATES
COMPLIANCE CHECKLIST**

The following applicable items should be listed as "met" before students can participate in any educational activities at Carle Foundation Hospital. Many of the requirements will necessitate pre-planning, communication and coordination with a Carle Foundation, Hospital Education Representative. Any required forms or Agreements should be sent to:

Carle Foundation Hospital
ATTN: Tammie Ellingson Manager of the Clinical Education Department.
611 W. Park St
Urbana, IL 61801

If you have any questions regarding this information, please call Tammie Ellingson at 217-383-4642..

| COMPLIANCE STANDARD | CLINICAL OR NON-CLINICAL STUDENT | COMPLIANCE STANDARD MET? |
|--|---|--------------------------|
| Submit <u>proof of</u> Immunizations- including TB Skin test within the last 12 months. Use attached form. | Applicable for all students & on-site faculty | |
| Complete and return your signed Confidentiality Agreement to Carle Foundation Hospital Education Department. | Applicable for all students and/or faculty | |
| Review Carle specific HIPAA Information. | Applicable for all students and/or faculty | |
| Review Carle Foundation Safety Information. | Applicable for all students | |

CARLE FOUNDATION HOSPITAL & AFFILIATES REQUIRED IMMUNIZATION & HEALTH STANDARDS

IMMUNIZATION REQUIREMENTS

- TB Skin Tests- within the last 12 months. Must be negative.
- Varicella (Chicken Pox)- History of chicken pox as a child meets immunization requirements.
 - Exceptions
 - Proof of immunity by titer or record of 2 live vaccinations is required of students whose educational experiences take them into Pediatric, Family Centered Care, Oncology or Neonatal Intensive Care Units.
- Rubella (German Measles)- Immunization or positive Rubella Screen or Titer.
- Rubeola (Red Measles)- Immunization or positive Rubeola Screen or Titer. Persons born prior to 1957 are considered to be immune. (Written documentation of: MD diagnosed infection, positive measles screen or documentation of receipt of 2 doses of live virus vaccine after January 1968 or on or after their first birthday)
- Mumps- Immunization in 1969 or later or MD diagnosed illness. Persons born before 1957 are considered immune. (Written documentation of immunization of live mumps vaccine at 12 months of age or later- after 1969).
- MMR (Measles, Mumps and Rubella) Immunization. (2 doses of MMR separated by one or more months and given on or after the first birthday eliminate the need for rubella, rubeola and mumps vaccination.)

We strongly recommend but do not require:

- dT- Booster every 10 years
- HBV- vaccination series
- Influenza vaccine- yearly

HEALTH STANDARDS

Please reschedule your time at the hospital if you are not feeling well or if you have any of the following:

- Fever > 100.4
- Conjunctivitis (pink eye)
- Diarrhea- lasting more than 12 hours
- Group A Strep- culture confirmed or physician diagnosed
- Jaundice- yellowing of the skin which might suggest viral hepatitis
- Cold sores (herpes)
- Active measles, mumps, pertussis, rubella or chicken pox
- Upper respiratory infection (cold)
- Tuberculosis and/or positive TB skin test
- Shingles (chicken pox) or any rash of unknown origin
- Head lice
- Scabies (mites that burrow under the skin causing a rash)
- Any draining wound such as an abscess or boil
- Impetigo (Type of skin infection)
- Mononucleosis



STUDENT IMMUNIZATION DOCUMENTATION

Student Name: _____

School Name: _____

Program/Course #: _____ / _____ Semester: _____

Students must provide written proof of immunization, infection or titer (including dates) for the following (copies of immunology records from the primary care physician may be attached):

TB Skin Test: _____ / _____
(within last 12 months) Date Given Result

Varicella: _____ (or) _____ / _____ (or) _____
(Chicken Pox) Date of #1 Injection Date of #2 Injection Date of Titer/Result Date of Infection

MMR (Measles, Mumps, Rubella):
2 MMR's OR 1 MMR and 1 Rubeola
_____ _____
Date of MMR #1 Date of MMR #2

Rubella - _____ (or) _____ / _____
Injection Date Titer Date Result

Rubeola - _____ (or) _____ / _____
Injection Date Titer Date Result

Mumps - _____ (or) _____ / _____
Injection Date Titer Date Result

Records have previously been submitted to Carle _____
Semester/Date

Medical Authorization given by: _____

Physician's Office Address: _____

(Phone) _____

-----For Staff Use Only-----

Cleared for clinical without restriction. Student needs proof of the following: _____
 Not cleared at present. _____

Immunization Review Completed _____

(Date)

Reviewed by: _____

**CARLE FOUNDATION HOSPITAL & AFFILIATES/SUBSIDIARIES (CFH)
STUDENT CONFIDENTIALITY AGREEMENT (AGREEMENT)**

HIPAA PRIVACY & SECURITY AWARENESS

I, (Print Name) _____, acknowledge that my signature below indicates the following:

1. I have received and will read the CFH-specific HIPAA Privacy and Security Awareness education documents.
2. I agree to abide by these standards and the related CFH policies and procedures designed to comply with the laws and regulations to protect the privacy and security of patient information.
3. I understand that, if, during the course of my assignment at CFH, I may be privileged to come into possession of confidential CFH business information including but not limited to financial, patient or employee information, that such information will be kept in the strictest confidence and will not be used or disclosed (shared) except for the sole purpose of my assignment at CFH.
4. I understand that photocopying of patient information is strictly prohibited.
5. I understand that I must ensure that any information that I am permitted to remove from CFH should not contain any individual patient identifiers (including but not limited to name, initials, address, clinic number, admission #, social security #, etc.) for identification purposes. In addition, I understand that the information should be disposed of in a secure and confidential manner to include but not be limited to shredding.
6. I understand that no patient, employee or other confidential business information is to be discussed in public areas such as hallways, elevators, shuttles, cafeteria or lobbies.
7. I understand that only authorized healthcare providers may divulge laboratory, medical or surgical findings to a patient or other authorized persons providing the patient has assigned consent.
8. I understand that the failure to follow the provisions of this agreement may result in my immediate removal from the observational, educational, clinical or non-clinical activity at CFH as well as civil and/or criminal penalties.
9. I understand that CFH reserves the right to revise, add, change and update the documents I received and related policies and procedures as may be required from time to time.
10. I agree to return this signed Agreement to the faculty member responsible for my CFH assignment *prior* to the start of the assignment so that it can be returned promptly to CFH.

Student Signature: _____

Name of School _____

Date Signed: _____

CARLE FOUNDATION



HIPAA PRIVACY RULES EDUCATIONAL PROGRAM CONTENT

INTRODUCTION TO HIPAA

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, includes the Standards for the Protection of Individually Identifiable Health Information – better known as the Privacy Rule. Most Health care providers must comply with the new requirements by April 14, 2003. The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records as well as other personal health information.

- ❖ It gives patients additional rights for more control over their information
 - ❖ It sets boundaries on the sharing of this information
 - ❖ It establishes appropriate safeguards that health care providers and others must achieve in order to protect this information
 - ❖ It holds violators accountable, with civil and criminal penalties that can be imposed if privacy rights are violated

The purpose of this program is to provide a *general* overview of the HIPAA Privacy Rule. Additional policies and procedures related to the Rule will provide further job-specific guidance. This job-specific training will be the responsibility of departmental leaders as these policies and procedures become available.

DEFINITION OF KEY TERMS

Protected health information, or PHI, is any information that individually identifies a person as it relates to health such as:

- Name
- Address
- Employer
- Relative's name
- Date of birth
- Telephone and fax #
- Email address
- Social security #
- Medical record number
- Member or account numbers
- Certificate #
- Voiceprint
- Fingerprint
- Full facial photograph
- Codes
- Driver's license number

And any other identifying characteristic, such as occupation, which may identify someone.

Treatment generally means providing, coordinating, & managing healthcare and related services. It includes referral to and consultation with other healthcare providers about healthcare and related services.

Payment generally means the activities undertaken by a healthcare provider to obtain or provide reimbursement for providing healthcare. This includes pre-authorization/pre-certification, utilization review, collection activities, billing, and other related activities.

Operations generally means activities such as QA, case management, training programs for students, auditing, legal review, business management, planning and development and other such activities related to our business as a healthcare provider.

Treatment, Payment and Operations may be referred to later during this session as T/P/O.

Use generally means sharing of PHI amongst 'Carle staff'.

Disclosure generally means the sharing in any manner of PHI with parties other than 'Carle' staff.

Generally, we are permitted to disclose PHI to Carle Clinic Association and HAMP staff for the purposes of T/P/O.

PERMITTED USES AND DISCLOSURES

Generally, you are permitted to use and disclose PHI for the purpose of treatment, payment and operations (T/P/O).

Other permitted uses and disclosures generally include:

- To business associates who are providing a service on our behalf
- As directed by a patient on a valid authorization form
- Those required by law (i.e. State reporting of births and deaths into databases)
- For judicial and administrative proceedings (i.e. in response to a subpoena)
 - For organ and tissue donation
 - For the purpose of Research
 - To avert serious threat to public safety

Refer to the policy on permitted uses and disclosures for the complete list.

THE AUTHORIZATION REQUIREMENT

For some of the permitted uses and disclosures, a written patient authorization is required. The Privacy Rule mandates that standard statements and elements be included in these forms.

Refer to our policy on Authorization for Release of Information forms for information about authorization requirements. Contact Health Information Management or the records custodian for the particular entity in which the records are maintained for assistance with regard to authorization forms.

THE MINIMUM NECESSARY RULE

Healthcare providers must make a reasonable effort to use and disclose only the minimum amount of PHI necessary to do their jobs. However, providers can disclose PHI requested by other healthcare providers if the information is necessary for treatment of a patient.

We are mandated by the Privacy Rule to define the minimum amount of PHI necessary by job class to perform job functions. Refer to your job description or contact your Manager for your specific PHI privileges.

RIGHT TO NOTICE OF PRIVACY PRACTICES

Patients have a right to adequate notice of all the ways we may use or disclose their PHI as well as our legal duties in protecting their information. We must make the notice available as follows:

- ❖ On the first treatment date even if the service provided is electronic
- ❖ As soon as is practical in an emergency treatment situation
- ❖ To those who ask for it
- ❖ On our web site
- ❖ Posted in a prominent location at all physical service delivery sites

We must make a good faith effort to obtain a written acknowledgement of receipt of the notice or document our good faith effort to attempt to obtain it except in emergency situations. These documents must be retained for a period of 6 years.

RIGHT TO REQUEST A RESTRICTION

Patients have a right to *request* a restriction on how we use and/or disclose their PHI:

- to carry out treatment;
- for payment;
- for our operations
- to others involved in their care; and/or
- when there is a request to notify family about patient information

According to our policy, requests must be made in writing. We are not required to agree to a restriction, but the entire organization must abide if we do agree to a restriction.

For example, a hospital patient is diagnosed with high blood pressure. He requests that his wife not be told about the diagnosis. It may seem easy enough to abide by this request to restrict. But following the policy is essential. There may be other departments that will see this diagnosis and disclose the information as part of their job functions unaware that you have agreed to a restriction. (i.e. the wife might see the diagnosis in the mailed billing statement).

Therefore, if a patient requests a restriction of uses or disclosures of their PHI, refer to the appropriate policy. Requests for restrictions will be handled by Health Information Management or the records custodian for the particular entity in which the records are maintained.

RIGHT TO ACCESS

Patients have a right to inspect and obtain a copy of most PHI about them. A request by a patient to view or receive a copy of PHI must be made in writing. These requests should be forwarded to Health Information Management or the records custodian for the particular entity in which the records are maintained.

RIGHT TO REQUEST AN AMENDMENT

Patients have a right to request an amendment to PHI. We are not required to agree to a request for an amendment to records.

According to our policy, these requests must be made in writing. Therefore, requests by a patient to amend their PHI should be forwarded to Health Information Management or the records custodian for the particular entity in which the records are maintained.

RIGHT TO AN ACCOUNTING

Patients have a right to request a report of certain disclosures that we make to outside parties. This does not include permitted disclosures for T/P/O, when a HIPAA compliant authorization to release information has been signed, or for disclosures made to the patient. Some examples of the disclosures we will need to include in such a report are:

- ❖ Disclosures **required by law** such as mandatory State reporting of:
 1. Deaths
 2. Births
 3. Suspected child or elder abuse
- ❖ Disclosures **for Public Health purposes** such as:
 1. Adverse drug events
 2. Tracking of medical devices
 3. Notification of a school of exposure to an infectious disease
- ❖ Disclosure for some Research activities

To determine which disclosures you make that need to be tracked, and how to track them, refer to our policy on Accounting for Disclosures.

According to our policy, these requests by the patient must be made in writing. If a patient requests a report of the disclosures we have made of their PHI, refer them to Health Information Management or the records custodian for the particular entity in which the records are maintained.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION

Patients have a right to request to receive communication of their PHI from us by alternative means or at alternative locations. We must accommodate reasonable requests. For example a patient may ask that the results of a lab test be called to their work phone number and not their home phone number. If a patient requests this from you, refer to our policy. For questions, contact the Privacy Official.

REASONABLE SAFEGUARDS

We must protect patient information from inappropriate disclosure. Some examples of policies related to reasonable safeguards that we have in place already include:

- ❖ Using locked recycle bins & shredders
- ❖ Keeping charts and records out of public view
- ❖ Logging off your computer and not sharing passwords
- ❖ Locking file cabinets with PHI
- ❖ Covering PHI when mailing
- ❖ Restricting conversations about patients to private areas

It is your duty to ensure that you follow these and any other current or new policies that will safeguard PHI routinely.

VERIFICATION OF IDENTITY

Before we disclose PHI, we have a duty to verify the identity of the person requesting the information. Refer to our policy for suggested methods to verify identity before disclosing PHI.

Some examples include:

- Asking for identification such as a driver's license
- Asking for information that the patient would know such as mother's maiden name, patient's middle name, or patient's place of birth

Refer to our policy on Verification of Identity for further guidance.

PATIENT COMPLAINT PROCESS

If a patient has a complaint or concern with regard to their privacy rights, they can be referred to the Patient Relations Department Actionline @ 383-3333 or to the Office for Civil Rights. The complaint process for patients related to privacy rights is, also, included in the Notice of Privacy Practices booklet.

EMPLOYEE COMPLAINT PROCESS

Every employee has a duty to report compliance concerns including possible breaches related to the privacy of PHI. Refer possible breaches related to the privacy of PHI to the Privacy Official, Carol Znaniecki, @ 383-7159, or call the Compliance Confidential Message Line @ 1-888-500-5012. Refer to Compliance Policy #608 for more information.

Retaliation against an employee for reporting compliance concerns will not be tolerated.

PENALTIES

Failure to comply with the Privacy Rule could result in civil and/or Federal criminal penalties including monetary fines up to \$250,000 and up to 10 years in prison. The Federal government is serious about protecting a patient's right to privacy of their information.

Therefore, Carle Foundation may impose disciplinary action for compliance related misconduct of its employees. Refer to the Human Resources Policy #408 for examples of such misconduct and the internal consequences.

SUMMARY

In summary, this program is a general overview of the HIPAA Privacy Rule and some of our related policies and procedures that apply to these Rules. You should refer to your specific entity, departmental and job-related policies and procedures as they would apply to this Rule.

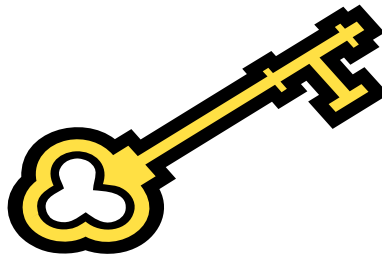
If you are faced with a privacy concern, refer to your resources:

- ❖ Our Policies and Procedures and your knowledge and good judgement
- ❖ Your leadership – use the chain of command to seek advisement
- ❖ Contact the Carle Foundation Privacy Official, Carol Znaniecki 383-7159
- ❖ FYI - Carle Clinic Association Privacy Official, Ron Sagritalo, at 326-8233

CARLE FOUNDATION



HIPAA SECURITY AWARENESS



Security Awareness – Protecting IT Assets

Learning Objectives:

- #1 Overview: Purposes of Security Awareness Program¹
- #2 Definition of Key Terms
- #3 What are IT Assets?
- #4 IT Security and Patient Privacy
- #5 Your Responsibilities
- #6 Consequences
- #7 Resources Available to You
- SUMMARY

Learning Objective #1: The Purposes of this Security Awareness Program

The purpose of this Security Awareness program is simply to:

- 1) Focus attention on basic Information Technology (IT) security principles because it makes good business sense to protect all our IT assets and business information as we move from paper to more electronic information;
- 2) Assist you in recognizing the importance of **your role** in securing the IT assets of the Carle Foundation-owned businesses (Carle); and to
- 3) Fulfill our obligations under the HIPAA Security Rule – federal law that imposes required IT standards to protect electronic patient information.

Q: ***But I don't use any computer or IT equipment to do my job at Carle. Why do I need to have this training?***

A: Even those employees, staff, volunteers, trainees and others who do not use any type of “computer” equipment to do their job are important links to a good IT Security program. For example, the failure to recognize and report suspicious activity or persons on Carle premises by any of its employees, staff or others could result in the compromise of IT assets.

As health care providers like Carle become more and more dependent on electronic systems to provide efficient quality care for our patients and to operate our businesses, the more important it becomes for us to protect our IT assets from incidents that could compromise that information. Think about the possible consequences to a patient if their medication orders were accessed, changed or deleted by an unauthorized person, or a virus that was introduced into that system.

A good IT Security Program that protects the reputation and integrity of our business depends on **ALL** of us.

Learning Objective #2: Definition of Key Terms

Assets = Something of value requiring protection (hardware, software, data, reputation)

Access = the ability or the means necessary to read, write, modify, delete, copy or communicate data or information or otherwise use any system resource

Availability = the property that data or information is accessible and useable on demand by an authorized person (see 3 parts of "Security" definition)

Confidentiality = the property that data or information is not made available or disclosed to unauthorized persons (see 3 parts of "Security" definition)

ePHI = protected health information in electronic format such as in software, hardware and other computer storage devices like CD's, diskettes, etc.

HIPAA Security Rule = part of the Health Insurance Portability and Accountability Act of 1996 that becomes **effective law on April 20, 2005**. Requires most health care providers like Carle to put into place standards for the protection of **electronic** patient information that it creates, receives, stores and transmits

Integrity = the property that data or information have not been altered or destroyed in an unauthorized manner (see 3 parts of "Security" definition)

Security = includes all 3 of the following terms (see definitions)

- **C** = confidentiality
- **I** = integrity
- **A** = availability

Security Incident = the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system (e.g. you receive an unusual email such as with an extension of .exe, you have frequent pop-up windows appearing on your computer, there is unusual slowness in performance of your computer, you suspect or know that your ID/password is being used by others, your computer, Personal Digital Assistant (PDA), laptop, text pager, etc. has been stolen)

Workforce = employees, volunteers, trainees, and other persons whose conduct in the performance of work for an entity is under the direct control of the entity whether or not they are paid by the entity.

Learning Objective #3: What are IT Assets?

Some examples of IT assets that may receive, store or transmit business information including ePHI are:

- Software and memory devices in computers (hard drives in personal computers, laptops, PDA's, biomedical equipment, blackberries, iPods, tablets, camera phones, cell phones, text pagers,ifax machines, etc.);
- Transportable electronic storage devices like CD's, magnetic tapes or disks/diskettes, optical disks, or digital memory cards; and
- Transmission media including the Internet, extranet, leased lines, dial up lines, & private networks.

Learning Objective #4: IT Security & Patient Privacy

A good IT Security Program will serve to better protect patient privacy. Here's why.

The HIPAA Privacy Rule requires standards for the protection of individually identifiable patient information including clinical, billing and demographic information – called protected health information or **PHI**. This protection is required for **all** PHI in **any** format including verbal (oral), written (paper), electronic, etc. that Carle creates, receives and maintains. Privacy laws lay the groundwork for basic protection of all PHI.

For example, the Privacy Rule requires Carle to identify those persons that should be granted the privilege to access PHI to perform their job duties - in other words "role-based access" based on a job description of duties. Only those persons that need access to perform job duties should have access. Carle's **Corporate General Policy #100.29** was created to comply with this regulation under the Privacy Rule. Access to patient information by workforce when it is not to perform a job duty – i.e. for personal reasons - is prohibited.

The HIPAA Security Rule requires additional protection for electronic PHI, or ePHI. Carle is required to put into place additional basic safeguards to protect ePHI from unauthorized access, alteration, deletion and/or transmission. These additional safeguards will help to support the privacy policies and procedures that we have already put into place to protect patient privacy.

For example, the Security Rule requires Carle to secure ePHI by assigning a unique user ID to each authorized user of an ePHI system. Those with a role-based need to access the system must have a unique user ID assigned to gain access. This Security standard reinforces the Privacy standard of role-based access.

Learning Objective #5 – Your Responsibilities

Every member of our workforce has a duty to protect Carle's IT assets. Your responsibilities are to:

- Use Carle IT assets for business purposes only and know and follow IT policies and procedures (found on the Cweb under the IT Department site)
<http://cweb.carle.com/IT/Policies/default.htm>
- Promptly report suspicious activity or persons on Carle property to the Security Department and your supervisor.
- Promptly report suspected or known IT security incidents to the IT HelpDesk at **383-4357** and your supervisor.
- Always safeguard your user IDs and passwords by **never** sharing them with anyone and **never** writing them down where someone may have access to them (e.g. **DO NOT** tape them to a computer monitor or inside a desk drawer that others can access).
- Guard against malicious software by downloading only Carle **authorized** software on to Carle IT equipment (e.g. use caution in downloading from the Internet or saving document attachments in email to the network from unfamiliar or un-trusted sources which can introduce viruses to our network)
- Monitor log in attempts and report anything unusual or issues to the IT HelpDesk at **383-4357**.
- Be wary of the "shoulder surfers" - others watching your key strokes as you log in
- Promptly report suspected or known viruses to the IT HelpDesk at **383-4357** (e.g. email like those with extensions of **.exe** or from an unusual or unknown source).
- Seek guidance from your chain of command (starting with your supervisor), the IT HelpDesk, or the Security Official if you have questions or concerns about IT security.

Learning Objective #6 – Consequences of Failure to Comply

The Carle Foundation is committed to protecting its IT assets and to following applicable laws, like the HIPAA Security Rule and copyright laws through its policies and procedures. Failure to comply could result in both internal and external consequences. Situations involving alleged misuse of IT assets will be thoroughly investigated, and actions will be taken on a case by case basis as deemed necessary based on the investigation results and Carle policy.

Internal Consequences:

Disciplinary action up to and including termination for failure to comply with policies and procedures could be imposed on employees. Refer to **Human Assets Resource Policy #408** for specific information.

Other workforce members besides “employees” such as independent contractors, temporary workers, volunteers, students, medical directors, etc. may be subject to internal consequences up to and including immediate termination of an encounter or relationship with Carle.

External Consequences:

Various civil money (\$\$) penalties and criminal penalties including possible jail time could be imposed on the individual and/or the organization by State and/or federal authorities as deemed appropriate to the circumstances and current laws (e.g. breach of contract and/or State and federal privacy, copyright and license laws).

Learning Objective #7 – Resources Available to You

There are many places to find more information about IT Security or to ask questions. Here are some of those resources:

- Carle Foundation Administrative Policies and Procedures Table of Contents Cweb site at http://cweb.carle.com/FoundationPolicies/Policy_TOC.htm
- IT Department Cweb site at <http://cweb.carle.com/IT/Policies/default.htm>
- Call the IT HelpDesk for questions at **383-4357** or **email questions to Help.Desk@carle.com**
- HIPAA Security Official (interim official for the Carle Foundation is Carol Znaniecki at 383-7159)
- Need policy help? If you don't have ready access to the Cweb, or just need help finding a policy, you can contact or visit the following locations to get assistance:
 - Educational Services in the basement of the Forum building
 - Human Resources in NT-1
 - Compliance Office in the RISK building just east of the hospital parking garage
- Check the Centers for Medicare and Medicaid Services web site under “Security Standards” at www.cms.hhs.gov/hipaa/hipaa2
- Check out the National Institute for Standards and Technology web site <http://csrc.nist.gov/publications/nistpubs/>

SUMMARY:





A good IT Security Program depends on **YOU**. Your commitment to know and do what's expected of you to protect IT assets will be the key to our success.


- Know and follow Carle Foundation policies and procedures.
- Report any Security Incidents to the IT HelpDesk and your supervisor.
- Seek assistance from available resources as needed.

**CARLE FOUNDATION HOSPITAL
OVERVIEW OF
SAFETY, PROFESSIONAL CONDUCT & SECURITY GUIDELINES
FOR
STUDENTS & FACULTY**

The following information is a mere overview of the safety policies and standards for Carle Foundation Hospital. Please review them and share the information with your students. When you arrive for your first educational day at Carle, please check with the Manager or Director for that area of the hospital for any unit specific safety information.




GENERAL SAFETY

| TOPIC | OVER HEAD ANNOUNCEMENT | INFORMATION & REQUIRED ACTIONS |
|---|---|---|
| FIRE  | Greenleaf & location = a suspected fire Greenleaf Alert & location = a confirmed fire | <ul style="list-style-type: none"> • Do not use the elevators in the same building as the alarm • Do not transport patients to the location of the alarm until a "Greenleaf all clear" is announced overhead. • Limit travel to & contact with the department/unit of the greenleaf alarm. • When you hear a fire alarm: <ul style="list-style-type: none"> ○ Close all doors in the department/unit. ○ Move patients & visitors out of the hallways and into rooms & lounges. ○ Clear the hallways of all equipment. ○ Search for the cause of the alarm. ○ Secure any important records (patient records) for a possible evacuation. ○ Instruct patients/visitors/staff not to block the hallway or use the elevators. • R.A.C.E when you discover a fire: <ul style="list-style-type: none"> ○ R- remove people from the fire scene, stay calm, walk & don't run. ○ A- alert Fire Dept by pulling the "red pull station" or Call 3-3911 to report a fire. ○ C- contain the fire and close all doors ○ E- extinguish the fire if smaller than the size of a trash can OR evacuate- follow direction of charge staff members and follow department/unit specific policy. |
| WEATHER  | Weather Alert Phase 1 = severe weather, secure area Weather Alert Phase 2 = tornado discovered, evacuate | <ul style="list-style-type: none"> • Weather Alert Phase 1 <ul style="list-style-type: none"> ○ Draw shades & drapes and remove loose items from the window sill ○ Lower patient beds to lowest position. ○ Stay clam & alert for further announcements. ○ "All clear" will be announced when conditions improve. • Weather Alert Phase 2 <ul style="list-style-type: none"> ○ Assist ambulatory patients & visitors to designated shelter areas in central corridors away from external windows & doors. ○ Close doors ○ If patients can not be moved, pull curtains around bed and place extra blankets over patient to protect from debris. ○ Clam patients & visitors, remain in the shelter area until "all clear" is announced. |
| HAZARDOUS MATERIALS  | NA | <ul style="list-style-type: none"> • MSDS- Material Safety Data Sheets- are information sheets on all chemicals. They list: <ul style="list-style-type: none"> ○ Proper handling techniques ○ Emergency response procedures ○ Emergency contact phone numbers ○ Full description of the chemical • Responsibility of students: <ul style="list-style-type: none"> ○ Know the location of the depart/unit MSDS binder ○ Read MSDS on chemicals before handling ○ Follow appropriate work practice as indicated by policy or the MSDS sheet ○ Dispose of chemicals appropriately as indicated on MSDS sheet ○ Ask faculty and or Carle mentor if you have questions or are unsure. |
| TOPIC | OVER HEAD ANNOUNCEMENT | INFORMATION & REQUIRED ACTIONS |
| INFANT ABDUCTION  | Code Pink | <ul style="list-style-type: none"> • Level 1 = abduction of an infant or child who is too young to walk. • Level 2 = abduction of a child who is old enough to walk. • Note any suspicious person or persons especially if they have an infant or child with them and immediately report it to Security 3-3911. • All employees are to follow their unit specific plans which will include: <ul style="list-style-type: none"> ○ Securing and manning all entrance or points of access to the complex ○ Search their area for the abducted infant, child or Abductor. ○ Look out windows and be aware of people around you. ○ Report anything to Security- 3-3911 ○ Do not make physical contact with abductor if confronted. Report to Security-3- |

| | | |
|---|----|---|
| | | 3911. |
| UTILITY  | NA | <ul style="list-style-type: none"> • All Life Sustaining and/or Life Support equipment that is currently in use on a patient MUST be plugged into a RED wall outlet. • RED outlets are supplied by the generator in the event of a utility failure. • In the event of any utility failure respond as directed by the Charge Nurse or Dept. Manager. • During an electrical outage: <ul style="list-style-type: none"> ○ Emergency generators will provide backup power within 10 seconds. ○ Ensure all critical equipment, especially life support equipment is plugged into a red outlet. ○ Emergency power will be provided to the RED outlets and RED wall switches only. ○ Minimal overhead lighting will be available. • Verify proper operation of all medical devices. |

INFECTION CONTROL

| | |
|----------------|---|
| GENERAL | <ul style="list-style-type: none"> • All your immunizations must be up to date. • Get your Hepatitis B vaccine. • Each job category is assigned a "risk category" based on the essential job duties of the position. The risk is assigned a Level. Level 1 = occupational exposure on a regular basis. Level 2 = some/occasional potential for exposure. Level 3 = little or no potential for exposure. • Know your risk level. • Understand the OSHA (Occupational Safety & Health Administration) Bloodborne Pathogen Guidelines. See below • Know where to find the Exposure Control Plan. • Use universal precautions at all times. This is a set of precautions from OSHA that mandates that all blood and body fluids be treated as if they were infected with a bloodborne pathogen. Universal precautions protect healthcare workers from exposure. • Wear personal protective equipment as indicated (Mask, Goggles, Gowns and Gloves). • Artificial fingernails (include but not limited to acrylic, overlays, tips or silk wrap) and fingernail jewelry ARE PROHIBITED. • DO NOT bend or recap needles or sharps. • Place contaminated or opened or used needles/sharps immediately and ONLY in an approved RED sharps container. • If there is not a sharps container readily accessible in your area and/or full, then report this to your instructor or mentor. • DO NOT eat in work or patient care areas. • Recognize the RED isolation & biohazard signs and follow them. • Report any injury and/or exposure to your instructor or mentor. |
|----------------|---|

| TOPIC | INFORMATION & REQUIRED ACTIONS |
|---|--|
| <p>OSHA</p>  | <ul style="list-style-type: none"> • 1991 OSHA (Occupational Safety & Health Administration) Standards on Universal Precautions states that any health care worker who might potentially come into contact with patients, procedures, specimens or items contaminated with blood/body fluids or tissue should be educated in infection control. • Treating ALL patients, specimens, procedures and items contaminated with blood and body fluids as if they could infect you with a bloodborne pathogen. • Examples of bloodborne pathogens include: HIV, Hepatitis-B or Hepatitis-C. • Potentially Infectious substances can include: <ul style="list-style-type: none"> ○ Blood- All human blood, blood components & blood products ○ Body Fluids- Semen, vaginal secretions, fluid around the heart, lungs, brain, joints or other organs in the abdomen, saliva, amniotic fluid or any other body fluids in situations where it is difficult to see blood or differentiate between body fluids. ○ Other potentially infectious materials- tissues, organs, cultures etc... that may contain blood or body fluids. • TB/Tuberculosis is an example of an airborne pathogen. TB can affect any organ or tissue but is mostly seen affecting the lungs. <ul style="list-style-type: none"> ○ Transmission occurs by inhaling the bacteria produced by people with the disease in their lungs during coughing, talking, singing or during certain invasive procedures. • Risk of infection is related to the duration and degree of exposure. A positive TB skin test does indicate that you have been exposed NOT that you have the disease- further testing is required to confirm diagnosis. • Other airborne pathogens include Varicella (chicken pox) and Rubeloa (Red Measles) • Some organisms are resistant to antibiotics requiring certain precautionary measures. Some examples include MRSA (methicillin or oxacillin resistant <i>staph aureus</i>) or VRE (vancomycin resistant <i>enterococci</i>). |
| <p>HANDWASHING</p>  | <ul style="list-style-type: none"> • Handwashing is the single MOST IMPORTANT activity to prevent the spread of infection! • Wash your hands after glove removal, before eating and after using the bathroom. • Wash your hands after every patient contact. • Remove gloves before leaving the patient's room or when finished with a patient related activity. No one else wants to be exposed to what you are protecting yourself from. • Avoid petroleum based hand lotions- they can damage latex gloves. |
| <p>TYPES OF ISOLATION</p> | <ul style="list-style-type: none"> • Patients can be under Airborne, Droplet or Contact Isolation. • The healthcare provider will need to comply with the isolation specific precautions: <ul style="list-style-type: none"> ○ Airborne <ul style="list-style-type: none"> ▪ Pt must be in a negative flow, private room. ▪ Caregivers must wear TB respirator mask (N-95). ▪ Caregivers MUST be fit tested by Employee Health or designee to be authorized to wear mask. ○ Droplet <ul style="list-style-type: none"> ▪ Pt should be in a private room ▪ Caregivers must wear N-95 mask ▪ Caregiver does not need to be fit tested before they can wear the mask for this purpose. Fit test is required for Airborne pathogens only. ○ Contact <ul style="list-style-type: none"> ▪ Wash with antiseptic soap- hibicilins ▪ Gown when touching patient • Equipment (including stethoscope) should be "dedicated" for this patient. This means the blood pressure equipment, stethoscope, thermometer etc... should not be shared with other patients to avoid the spread of infection or colonization. |
| <p>GOOD HOUSEKEEPING</p>  | <ul style="list-style-type: none"> • Housekeeping is everyone's responsibility. Keep your work areas clean and safe. • Many people handle the trash once you are through with it- we want to keep everyone safe. • Trash <ul style="list-style-type: none"> ○ Effectively and appropriate dispose of trash and linens. ○ Put any sharp object in the sharps container. ○ Ensure trash bags are double tied shut. ○ Biohazard waste goes in only RED biohazard trash bags. ○ Do not throw non-biohazard materials in biohazard bags- this helps to keep waste disposal costs down. |

| TOPIC | INFORMATION & REQUIRED ACTIONS |
|-------|--------------------------------|
|-------|--------------------------------|

GOOD HOUSEKEEPING CONTINUED

- Linen
 - ALL soiled linen is considered infectious.
 - Linen from isolation patient rooms is handled in the same manner as other linen.
 - ALL soiled linen is to be placed in a clear bag, double tied and taken to the soiled linen cart.
 - Do not overfill the linen bags- you will need to carry it.
 - Do not place linen in any other colored bag besides clear.
- Equipment
 - Clean equipment regularly.
 - Hospital approved disinfectant is available and should be used on all items in between patients.
- Some equipment can be re-used and should be sent to Sterile Processing Department for reprocessing.

PERSONAL CONDUCT



- While at Carle Foundation Hospital you are not only an acting representative of your school but of Carle Foundation as well. Many visitors and patients are not aware that you are a student. Your actions or lack thereof can effect the views and opinions of our patients and visitors.
- During your educational experience at Carle, you are under the supervision of either a school faculty member or a Carle appointed mentor/preceptor.
- While at Carle, we expect that:
 - You dress according to your schools policy. This should include NO: hats, jeans, shorts, sandals, sport team shirts or tank tops.
 - You perform daily personal hygiene.
 - Your hair is clean, fastened securely (if long). Beards and mustache should be clean and neatly trimmed.
 - Fingernails should be of reasonable length and trimmed. No artificial nails or nail jewelry is permitted.
 - Perfume, cologne or scented lotions should not be worn or used if performing patient care.
 - Jewelry should be conservative.
 - Your ID badge is worn at all times
 - You not use stethoscope covers- they can be a source of infection. Latex free stethoscope is recommended.
 - Refrain from using profanity or from raising your voice.
- Some Customer Service expectations include but are not limited to:
 - Use the stairs when possible. Especially if you are physically able and you are going either 1-3 flights up or down.
 - When the elevators are needed to transport a patient, please step off the elevator and take the next one and/or use the stairs.
 - Pick up trash or liter in patient care areas or hallways.
 - Park in the Fairground designated parking lot and use the shuttle on weekdays. Refrain from parking in visitor parking garages on weekdays. The shuttles do not operate on weekends. On weekends, you can park in the parking garage for free.
 - If visitors appear lost or looking for something, please assist even if you are not sure. Find someone who can help them. It's always best to escort visitors to the area they are looking for rather than giving directions.

SECURITY



- Do not bring valuables or large amounts of money to Carle.
- Secure your valuables.
- Use the Carle supplied shuttles- especially at dusk or at night.
- You can request for an escort if arriving or leaving after the shuttle hours of operation. Call Carle security for an escort- 383-3122. Operating hours for the shuttles are weekdays 5:00am –9pm.
- Pay attention to your surroundings.
- If you need to report a theft or crime while at Carle, call the Carle Security Office at 383-3122.