LIFE SAFETY MANAGEMENT

INTRODUCTION/VALUE STATEMENT:
UPMC Horizon has developed the Life Safety Management Program to protect patients, personnel, visitors, and property from fire and the products of combustion, and to provide the safe use of buildings and grounds. This packet is designed to provide the basic information you should know regarding the Life Safety Management Program. Life Safety Management is part of the JC Standards for the Environment of Care and may be found in Chapter V of the Environment of Care (EOC) Manual.

OBJECTIVES:
After completing this packet, you will know the following:
✓ The use and function of the fire alarm system.
✓ Procedures to contain smoke and fire.
✓ Your responsibility when at the fire’s point of origin.
✓ Your responsibility when away from the fire’s point of origin.
✓ Where to obtain department specific fire safety information, including evacuation plans.
✓ Definition and purpose of ILSM (Interim Life Safety Measures).

Life Safety
Fires can be devastating to life and property. Knowing what to do in the case of a fire is extremely important in the hospital environment. Not only your own lives, but the lives of patients and visitors rely on quick and responsible actions. The Life Safety Management Program has been prepared to acquaint all Hospital personnel with their individual responsibilities in the event of a fire.

What to do if there is a Fire:
Knowing what to do before a fire occurs will help in eliminating some of the anxiety acquainted with fire response. Here are some basic fire safety points:

- Report ALL fires and locations, no matter how minor.
- Keep calm, do not panic or shout. Fear can do more harm than the fire.
- Know where the following are located in your area:
  * Fire alarm box (pull station)
  * Fire extinguishers
  * Next compartment for relocation of patients and staff (next smoke or fire barrier)
  * Oxygen shut-off valves

  CAUTION: After receiving clinical approval, Oxygen should be shut off when it is determined to be an immediate threat to life safety.

  ➢ Know the Hospital fire code: “CODE RED”.
The person in charge of the department will be in command of the scene pending the arrival of the Fire Response Team and/or the Fire Department.

- Don’t use elevators! Use the stairs.
- Do not make unnecessary telephone calls, this only ties up the lines.

**Reporting a Fire:**
To report a fire, follow these procedures:

1. Pull the nearest fire alarm box (pull station).
2. Dial “5511” at the Shenango Valley Facility and “5555” at the Greenville Facility.
3. Be sure to give your name, the location and the extent of the fire. This is in addition to pulling the fire alarm.

**Use and Function of the Fire Alarm System:**
The alarm pull stations are conveniently located on the walls near the exits in every area of the hospital. The following will happen upon activation of the alarm system:

- All fire alarm response systems will be activated. Fire and smoke doors will close to contain fire or smoke.
- The alarm will sound and the bell pattern will indicate the location of the fire. (Listings for the bell-codes are located on the walls throughout the hospital).
- The switchboard operator will announce the **“CODE RED”** and the location of the alarm.
- Local fire companies will be alerted via 911.
- All smoke and fire doors will close automatically.
- All personnel will initiate the appropriate fire procedures.

**Fire Drills**
Fire drills will be conducted at each campus at least once per shift *per quarter*. All personnel are asked to cooperate and conduct themselves as though an actual fire exists.

**Fire Response - Point of Origin:**
JC Standards require you to be familiar with your responsibilities if you are at the point of origin of a fire. Protecting the safety of patients and fellow workers depends on you knowing the correct procedures. The following procedures have been developed for that purpose:

Any patient in immediate danger is removed from the room of fire origin, and all doors to the corridor are closed.

The person discovering the fire sounds the alarm or, while removing the patient, assigns a co-worker to sound the alarm. A call to the operator (“5555” – Greenville Campus) / (“5511” – Shenango Valley Campus) should also be made simultaneously in order to confirm the location of the fire. This action will:

- notify the fire department
- alert personnel throughout the hospital
Persons are evacuated from the threatened area, if needed. Patients in the immediate area of
the fire or in danger should be moved to safety immediately. Begin with any patients in the
room containing the fire, then evacuate or remove of patients in the adjacent rooms,
continuing until the immediate area is evacuated. Patients should first be evacuated
horizontally on the same level behind the nearest smoke or fire door. Vertical evacuation
will occur if ordered by the Fire Response Team. And/or the Fire Department.

To evacuate the immediate area of the fire, patients confined to bed should be evacuated in
the bed, if possible, transferred to a carrier, or carried to safety. Patients able to be moved
by wheel chair should be wrapped in a blanket and pushed to safety. Ambulatory patients
should be wrapped in a blanket and led to safety. The evacuation of patients in the
immediate area of the fire must be done quickly but calmly, and does not require the order
of the Fire Response Team or Fire Department.

Should a fire occur in a patient bed, smother the flames with a pillow or blanket, remove the
patient from the bed, then all patients from the room. A hand extinguisher, or even a
pitcher of water or wet blanket, can be used to smother small fires (Use caution and
common sense in deciding to fight a fire).

After the patient(s) has been evacuated from the room, other electrical equipment should be
shut off. Oxygen should be shut off if in use after receiving clinical approval. All windows
and the doors should be closed.

If fire hoses must be used, Maintenance, Security and/or the fire department will be the only
departments authorized to utilize these hoses.

Utilities, such as gas, oxygen, and ventilating equipment, are controlled or shut-off. Utility
“shut-offs” will be handled by the Maintenance Department. In the case of immediate
danger, any employee at the fire’s point of origin may shut off the utilities after receiving
clinical approval. Be sure to secure patient care!

Control of activities is turned over by the Fire Response Team to the fire department upon
arrival.

**Fire Response - Away From the Point of Origin:**
If the fire alarm sounds, and the bells indicate that the fire is in another department, you still
have responsibilities. The following procedures have been developed in compliance with JC
Standards under the Environment of Care for response to fires away from point of origin:

1. Insure the calm and safety of all patients, visitors, staff, etc.
2. Ask all patients and visitors to remain in their rooms.
3. Turn off all unnecessary lighting, electrical appliances, etc.
4. All doors and windows must be closed.
5. Check all ceilings, floors, stairways, etc. for any sign of smoke or fire.
6. Do not leave your area/floor, unless absolutely necessary, and never go to the scene of the fire, unless directed to do so.

R.A.C.E.:
UPMC Horizon uses the acronym R.A.C.E. to assist employees in remembering the fire policy procedures.
- R: Rescue people in immediate danger.
- A: Pull Alarm (call the operator and confirm location).
- C: Contain fire and smoke by closing all doors.
- E: Extinguish and evacuate (use good judgment).

“No Smoking”
The most common cause of a fire is careless smoking and the careless mishandling of smoking materials. The hospital prohibits the use of smoking materials throughout its buildings and grounds. UPMC Horizon is a non-smoking facility.

Use of Fire Extinguisher
- Before you decide to fight a fire make sure the fire is confined to a small area and that it is not spreading beyond the immediate area.
- **Always** make sure that you have an unobstructed escape route between you and the fire.
- Make sure that you have read the instructions and know how to use the extinguisher. It is reckless to fight a fire under any other circumstances. Instead, leave immediately and close off the area.
- Be sure you have the right type of extinguisher for the fire. The flyer on the next page explains the different types of extinguishers for different types of fires.

Knowing when to fight a fire and what extinguisher to use will not help you if you don’t know how to use an extinguisher. UPMC Horizon has adopted the acronym **P.A.S.S.** to help its employees remember the procedure to correctly use a fire extinguisher. Remember to stand 6 to 8 feet away from the fire and follow the four steps of **P.A.S.S.** If the fire does not begin to go out immediately, leave the area.

- **P**ull the pin between the two handles.
- **A**im at the base of the fire – If you spray the agent directly into fire, the pressure may spread the burning materials.
- **S**queeze handles together.
- **S**weep from side to side. Evenly coat entire area of the fire.

**Department Specifics:**
Every department should supplement this plan with department specific steps and procedures. Evacuation plans should be tailored to the area. If you have any questions, ask your supervisor.

**Fire Extinguishers:**
Small fires can be contained and extinguished before they can cause damage to persons or property if the right fire extinguisher is used. Fires are rated: A, B, C, or D, depending upon the type of “fuel” that is burning. Fire extinguishers are rated according to the type of fire that they can put out. This information is listed prominently on the extinguisher. Take a moment to learn the four types of fires so that you’ll know which extinguisher to use if you find yourself in a fire emergency.

**Fire Extinguisher Codes:**
Fire extinguishers come in many varieties – water, carbon dioxide, dry chemical or powder, and liquefied gas. Fire extinguishers are coded to reflect the type of fire they can put out: A (green label), B (red label), C (blue label), D (yellow label). Newer extinguishers have picture codes showing the type of fires they can be used on.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| A-B-C | Wood, paper, cloth, rubbish  
Flammable gas/liquids  
Electrical fires |
| B-C | Flammable gas/liquids  
Electrical fires |
| K | (For use in kitchen areas)  
For grease fires |
| Halon | For grease & electrical fires |

**Types of Fires**

Be sure to use the right extinguisher for the type of fire you are confronting. Using the wrong extinguisher can actually make the fire worse.
PRIVACY AND SECURITY AWARENESS

Numerous federal and state laws require that UPMC protect information that is created or collected for a variety of purposes, including patient care, employment, and retail transactions. Education and training is a key element of an effective compliance program. The Privacy and Security Awareness training is an example of UPMC's commitment to educate and promote a culture that encourages ethical conduct and compliance with applicable laws.

After completing this course you should be able to explain:

- your obligations regarding privacy
- your responsibilities for protecting information
- what you should do in the event that you suspect that a breach may have occurred

Additionally, you should become familiar with the UPMC policies that discuss these subject matters. All policies that are mentioned in this course will be reviewed from time to time and may change. It is your responsibility to periodically check these and become familiar with any changes or updates.

What is Privacy and Security?
Privacy is UPMC's obligation to limit access to information on a need-to-know basis to individuals or organizations so that they can perform a specific function for or on behalf of UPMC. This includes verbal, written, and electronic information.

1. **Security** - ensure that only those who need to have access to information can access the information. Security also includes ensuring the availability and integrity of information.

2. **Need-to-know basis** - information should only be provided to those that need it to perform their assigned job responsibilities.

Complying with UPMC Privacy and Security Policies
As an employee you are to comply with UPMC's Privacy and Security policies and procedures. To increase patient confidence, and ensure that information is protected at UPMC, all employees are required to:

1. Abide by UPMC policies and all applicable laws
2. protect patient privacy
3. safeguard confidential information
4. read and understand policies related to their job function

Every employee must respect our patient's expectations that their information will be kept confidential.
Consequences for Violating Privacy and Security Policies
Employees who violate any UPMC policy that supports compliance with HIPAA regulations may receive disciplinary action, up to and including termination.

1. The United States Department of Health and Human Services has appointed government agencies to enforce HIPAA compliance. Those who violate HIPAA can face the following penalties:
   - individual fines of up to $250,000
   - imprisonment up to 10 years

What is PHI?
Protected health information (PHI) includes any health information about our patients and is considered confidential. PHI can include, but is not limited to:

General information:
- patient's name
- medical record number
- social security number
- address
- date of birth

Health Information:
- diagnosis
- medical history
- medications

Medical coverage information

Dental coverage information

Safeguarding Information
You are only permitted to access and use patient information as it relates to your job. If you see or hear patient information in the course of doing your job, that you do not need to know, remember that this information is confidential. You are not permitted to repeat it or share it with others - even friends, family, or other employees who do not have a need to know it.

- Additionally, you are not permitted to share this information with others when you no longer work for UPMC.
• All UPMC staff members play an important role in safeguarding sensitive information.
• You are obligated to maintain a patient’s privacy and safeguard protected health information (PHI) for anyone who receives services at UPMC facilities.

Information Without Safeguards
An unauthorized individual may be able to gain access to information if sufficient safeguards are not in place. This information may reveal confidential patient, staff, financial, research, or other business information.

Places where this type of information may be accessed:

- computers that were left logged into
- overheard in cafeterias or hallways
- found on fax machines and/or printers
- found in a wastebasket
- seen lying on a desk or counter

And it could be used in an inappropriate manner to:

- reveal confidential information
- sell information to a tabloid
- cause negative publicity

If this occurs:

- A patient’s privacy rights may have been violated.
- State and federal laws may have been violated.
- UPMC and associated staff may be responsible for damages.

Potential Threats or Activities that May Compromise Information
There are many ways that confidential information can be inappropriately accessed or disclosed. All must be reported to your manager or Privacy Officer.

These may include:

• unauthorized access to information, either by an unauthorized individual or by an individual who has the right to access to information, but accesses the information for unauthorized reasons
• computer viruses
• inappropriately deleting information
• during a burglary, paper information may be accessed or duplicated
- theft of computer equipment, records, and/or information
- unauthorized disclosure of information

**Oral Communication**
Confidential or sensitive information should only be communicated or accessed on a need-to-know basis. You should access only the minimum amount of this type of information needed to perform your job.

**You can maintain privacy by:**

- disclosing confidential information only to those who have a need to know it
- speaking in an appropriate tone of voice (lower your voice when others are nearby and may be able to overhear your conversation)
- moving the discussions to areas where others cannot overhear
- asking those around you who do not need to know this information to leave the area so you may have privacy
- not conducting conversations which include confidential information in high-traffic areas such as hallways, reception areas, waiting rooms, elevators, and cafeterias.

**What Should You Do?**
A health care employee was using a cellular telephone when discussing protected health information (PHI) in a restaurant down the street from the hospital. Another hospital employee sitting nearby overheard the conversation and approached the individual.

**The right thing to do . . .**

- Employees should never conduct hospital business and discuss confidential information in public areas.
- All hospital employees have the responsibility to abide by hospital policies and to protect patient privacy.
- Protecting patient privacy is an expectation of all employees whether on duty or off duty.
- If you overhear others discussing confidential information, let them know that they can be overheard.
- In any event, any information that you overhear should not be repeated or communicated to others.
- You should report inappropriate incidents or situations to your hospital's privacy officer.

**Physical Security**
Simple measures can be taken to prevent an unauthorized individual from gaining physical access to confidential information.
These measures include:

- Question individuals you do not recognize if they are in or near areas that contain confidential information.
- Offer assistance to those who may be lost.
- Keep file cabinets, doors, and desks locked in nurses’ stations, offices, etc.
- Insist that all repair/maintenance personnel show proper identification if they arrive in your work area to service equipment. If necessary, call the service company to have the identity of the repair or maintenance personnel confirmed.
- Accompany visitors and repair/maintenance personnel to and from their destinations.
- Notify Security when there is an unauthorized individual in a secured work area.
- Restrict access to computers and data centers to prevent unauthorized individuals from accessing electronic information.
- Ensure that any vendor representative, especially from the pharmaceutical, biotechnology, medical device, and hospital equipment industries, has registered with UPMC Supply Chain Management before they appear onsite.

**Photocopiers**
When making copies of confidential information, you should not leave the copier until your job is complete.

Additionally, employees should:

- Remove all papers containing confidential information.
- Check all areas of the photocopier, including the output tray, the input feeder, and the top of the glass surface.
- Not allow others to see the information that you are copying. If someone is standing close enough to see this information, advise him or her that you are copying confidential information. Offer to let the person know when you are finished so that he or she may come back to use the machine.
- Destroy or return any confidential information that has been left on a photocopier to the owner.

**Fax Machines**
The faxing of protected health information (PHI) should be performed only when absolutely necessary. Other, more secure ways of sending information should be considered (i.e., secure e-mail, registered/insured mail, etc). When you are asked to fax information to a UPMC
location, determine if they can access the information electronically which would eliminate the need to fax the information.

If you must fax, you are required to use the UPMC approved standard fax cover sheet. This sheet contains your contact information and a confidentiality disclaimer. This form can be found on the Infonet Quick Links tab under Forms.

Additionally, employees should:

- When possible, program automated dial buttons with frequently dialed fax numbers.
- If available, use the button on the fax machine to dial pre-programmed number for the receiving party.
- Confirm the fax and telephone numbers of the person you are faxing to.
- Prior to faxing confidential information, let the person you are faxing to know so he or she may retrieve it from the fax machine immediately.
- Follow up with the person to verify that he or she received the fax.
- Immediately remove confidential information from the fax machine.
- Destroy or return any confidential information that has been left on a fax machine to the owner.
- Destroy confidential information that has been received in error and advise the sender of the error.
- Periodically verify that pre-programmed fax numbers are still correct.
- Contact the privacy officer to report inadvertent faxing to the wrong person.
- Consider using other means as opposed to faxing.

**Disposal of Confidential Information**

Never discard paper, computer disks, or other portable media that contain patient information in a "routine" wastebasket. This makes the information accessible to unauthorized personnel. Such confidential information should be discarded in accordance with your business unit’s policies regarding the destruction of protected health information.

- Always shred or dispose of confidential information in an appropriate designated container.
- Check with your manager or supervisor to find out how your department disposes of confidential information.

**News Media Inquiries**

The news media may contact your facility for information if a well-known person or someone involved in a newsworthy situation, such as an accident, is being treated at your facility.

- Direct all news media inquiries to UPMC Media Relations.
Report Inappropriate Use of Patient Information

If you feel that a patient's privacy or confidentiality has been violated, report the incident to your facility's or business unit's privacy officer. If they are unavailable or you are not comfortable reporting it to them, you can also use the following options:

- UPMC HIPAA Program Office at 412-647-5757
- Compliance Helpline (anonymous option) toll-free at 1-877-983-8442.

Protecting Electronic Information

- Every UPMC staff member plays an important role in protecting UPMC's electronic patient, business, personnel, academic, and research information. Staff shall take reasonable precautions to ensure that electronic information is available, has integrity, and is secured against unauthorized access.

Creating and Protecting Passwords

A password is a unique combination of letters, numbers, and symbols that you use to verify your identity in a computer system. Your password is the electronic equivalent of your signature.

- Do not share your password with anyone (this includes your boss and the information technology staff).
- You are responsible for all actions performed under your username and password.
- Treat your password as you would treat any piece of personal and confidential information by taking measures to keep it confidential.

You are responsible for any activity that takes place under your username and password.

Creating Complex Passwords

Knowing how to create a complex password (one that cannot be guessed easily by someone else) is one way to protect your password.

- Don't base your password on information that is commonly known about you, such as your birth date, the names of your children or pets, or a hobby.
- It's also best to avoid common words, such as mother or father.

Passwords should meet the following requirements:

- must not contain all or part of the user's account name
- must be at least seven characters long
• must contain characters from three of the following four categories:
  o uppercase characters
  o lowercase characters
  o numbers, 0-9
  o non-alphanumeric characters (!, #, %, *, )

Examples:
I love to golf! = Iluv2GLF!
Opera singer = Opra$Ingr
I owe you $44.95 = iOu$449

Protecting Your Password
Once you've selected a complex password, follow these tips to keep it confidential:

• Don't share your password with anyone.
• Memorize your password.
• Never store your password in a computer file or PDA.
• Do not keep a written password in plain view or easily accessible to others. All written passwords are to be kept secured.
• If someone learns your password, you should immediately:
  o change your password
  o tell your supervisor and privacy officer

Remember, you are accountable for any actions made under your username and password.

Protecting Your Computer from Viruses
A virus is a computer program that performs unexpected or unauthorized actions. A virus can occur without your permission or knowledge. Viruses threaten all types of information, can render a system unavailable, and corrupt information contained in a system.

A virus might:

• expose or change confidential information
• delete or remove important files
• display unusual messages
• e-mail everyone in your address book
• disable computers
• spread to other computers
**Signs of a Computer Virus**
Contact the ISD Help Desk at 412-647-HELP (4357) or the help desk for your UPMC facility if you notice any of the following which might indicate your computer is infected with a virus:

- antivirus software pop-up alerts
- missing files
- unusual activity (for example, programs opening that you did not open)
- responses to e-mails that you did not send
- drastic, unexplained reductions in your computer's memory or disk space

**Preventing Viruses**
Precautions that you can take to help protect your computer from becoming infected with a virus are:

- Never open or run unexpected e-mail attachments or other programs.
- Always use antivirus software and never disable it.
- Scan all e-mails and downloads.

**Appropriate Use of E-mail**
Electronic mail (e-mail) is provided for the purpose of conducting UPMC business and providing service to our customers. Appropriate use of e-mail can prevent the accidental disclosure of confidential information and the disruption of computer services.

As an employee:

- Use e-mail only for official UPMC business and in accordance with UPMC policies.
- Do not use e-mail in a way that is disruptive, offensive, or harmful.
- Do not use e-mail to sponsor or promote a political party or candidate or to campaign against a political party or candidate.
- Do not use e-mail to solicit employees to support any group or organization.
- Confirm destination of e-mail addresses you are sending to.
- Do not use "reply all" unless necessary.

Although it is delivered electronically, e-mail is still a written form of communication. Approach it as you would other forms of written communication, such as a memo or fax.

**You should:**

- Delete unnecessary e-mail.
- Use additional security methods when sending confidential information.
- Include a confidentiality disclaimer on e-mails.
- Don’t write something in an e-mail that you would not say in an official memo.
Printers
Because many employees often share one printer, it is necessary to take measures to protect confidential information when printing.

Follow these steps:

- If your business unit has a Xerox multi-function machine you should use the "Secure" printing option. This means the document will not print until you release it by entering a code number that you select.
- If your business office does not have a Xerox multi-function machine then you should retrieve your documents immediately.

No matter what type of machine you are printing to, you must:

- Confirm to which printer you are printing, especially if you share a network printer.
- Immediately remove confidential items.
- Cancel or retrieve any confidential information printed on the wrong printer.
- Deliver or dispose of confidential information found on a printer.
- Only print what is necessary if you need to maintain a hard copy.

Internet Use
The Internet is a great source of information and a way to improve business efficiency. UPMC provides Internet access to facilitate business and for educational purposes.

- Do not use the Internet in a way that violates UPMC policies.
- Do not download software that is not approved for UPMC computers, including screen savers and games.
- Do not view information that is offensive, disruptive, or harmful to morale.
- Use antivirus software.

Proper Computer Workstation Use
Be sure to restrict the view or access of others by positioning your computer screen so that others cannot view it. Place your computer workstation in a secure area that is not easily accessible by unauthorized personnel. Make sure your screen saver is set to automatically activate and lock your computer and hide confidential information when your computer is not in use. If you cannot restrict others from viewing your screen, ask your manager to order a privacy screen for you that will be placed over your monitor. The privacy screen prohibits people who are not directly lined up to the monitor from viewing the information on the screen.

Employees should:
• restrict views of others
• place computers in secure areas
• use automatic screen savers that lock your computer

Log on and sign off procedures
Follow appropriate log on and sign off procedures. Follow these guidelines even when you are remotely logging into the UPMC system and accessing confidential information.

• Never use someone else's username and password or allow someone else to use yours.
• Don't offer to sign onto a computer so someone else may use it.
• Prevent another person from using your sign-on by locking or signing-off your computer workstation when leaving it unattended.
• To lock your workstation, press control/alt/delete, and select lock computer.
• Look away when other individuals are entering their passwords.
• Log off a computer when no longer using it.

Confidential Information Storage
Do not store sensitive and confidential patient information on local computer workstations (C Drive), laptops (C Drive), and mobile devices such as, flash drives or memory sticks unless you are authorized to do so. Instead, store information on your network shared drive or departmental shared folders.

• If you are authorized to store sensitive and confidential patient information on removable media such as, CD-ROMs, DVDs, floppy disks, flash drives, or memory sticks, then you must secure this removable media by keeping them in a locked drawer or cabinet.
• Delete files that are no longer needed.

Software installation/removal procedures
Follow software installation and removal procedures:

• UPMC must own a valid software license for all software installed on its computers.
• Unlicensed software shall be removed or a valid license shall be acquired immediately.
• Don't download software that is not approved for UPMC computers.
Technical Support
Seek technical support when necessary, especially when installing and removing hardware or software. Do not attempt to fix computer-related problems yourself. You may cause more difficulties by attempting to resolve the problem on your own. Contact the ISD Help Desk at 412-647-HELP (4357) or the designated help desk for your facility about any technical support problems or questions. Do not install or remove hardware - for example, modems, sound cards, video cards, or CD-ROMs yourself. Submit a request to complete the project.

- Seek technical support for hardware installation and removal.
- Do not attempt to fix computer problems.
- Do not install or remove hardware.
- Contact the Help Desk for technical support at 412-647-HELP (4357).

Remote Access Procedures
UPMC offers ways to access its network resources from off-site (remote) locations. Regardless of where you access information, remote or on-site, this information must remain confidential and secure. Follow established remote access procedures. Contact your Help Desk to discuss these solutions.

- You should not install any hardware, such as a modem or software used for remote connections, on a UPMC computer.
- Always contact your Help Desk for this service.
- Use approved solutions for accessing UPMC's network.
- Do not install any hardware that would allow remote connections.

Laptops and PDAs
Laptops and personal digital assistants (PDAs) often contain confidential information. Therefore, all staff should take the following security measures. Contact the ISD Help Desk with any questions.

- Physically secure laptops and PDAs.
- Use a password.
- Encrypt information.
- Do not leave a laptop or PDA unattended in a public place.
- The use of any unsecured wireless network is not allowed, unless the appropriate approval has been obtained.
- Confidential information should not be accessed without approval.
Disposal of Electronic Media
Electronic media must be disposed of properly.

- Floppy disks, CD-ROMs, DVDs, and backup tapes containing confidential information should be physically destroyed.
- This can be done by using a CD-ROM shredder or placing the items in designated shredding bins, which is the preferred method. Caution: The process of manually breaking a CD-ROM can cause sharp pieces of plastic to fly through the air.
- Special measures must be taken to remove confidential information from fax machines, copiers, printers, and other devices capable of data storage.
- Contact the ISD Help Desk at your facility to have the appropriate technical support staff remove all traces of confidential information from a computer hard drive and other devices.

UPMC Privacy and Security Policy Overview
You are required to understand all UPMC privacy and security related policies. This section provides an overview of these policies. In addition to these, your business unit or facility may have additional privacy and security related policies or procedures. If you do not understand a policy or procedure, ask your manager for clarification.

Some forms such as the Authorization for Release of PHI, have been updated in accordance with applicable regulations.

UPMC Privacy and Security Related Policies
UPMC developed privacy and security policies that address a variety of topics. Summaries of these policies are on the next several pages. The complete text of these policies can be found in the system-wide policy manual located on Infonet.

Release of PHI
Strict rules apply to the release of protected health information (PHI) when necessary for reasons other than treatment, payment, or health care operations (TPO). These rules vary based on the sensitivity of the information. Please direct questions related to releasing patient information to your HIM department or your privacy officer.

- If you are involved with disclosing PHI, you are responsible for being aware of these rules.
- Generally patients must sign an Authorization to Release their PHI if for reasons other than TPO.
- If a patient pays for services out of pocket in full and supplies in writing their request that we do not share this information with their insurer we are not to release this information.
A valid authorization must contain certain information.

**Notice of Privacy Practices for PHI**

The Notice of Privacy Practices is to be posted and made available in public areas of health care facilities, such as a registration area. The notice also must be given to patients during their first visit to UPMC and offered each additional time a patient registers for services. Patients should acknowledge that they have received a copy of the notice. At UPMC, patients acknowledge they have received the notice by signing the Consent for Treatment Form. If you are unable to obtain a patient's acknowledgement, you must document the effort and the reason why the acknowledgement was not obtained. During emergency situations, the acknowledgement should be obtained within a reasonable amount of time.

- All staff should read the Notice of Privacy Practices. The notice may be downloaded from the HIPAA section of UPMC Infonet.

**Notice of Privacy Practices (NOPP) describes:**

- how PHI may be used or disclosed
- patient rights under HIPAA
- who to contact if patients believe their rights have been violated

**Business Associates (Guidelines for Purchasing)**

A business associate is an external individual, business, or vendor that uses Protected Health Information (PHI) to perform a service or provide a product on behalf of UPMC. These services may include, but are not limited to, legal, actuarial, accounting, consulting, management, administrative, accreditation, data aggregation, or financial services.

- UPMC is required to enter into a contract with a business associate that clearly defines the business associate's responsibilities for using, sharing, and safeguarding PHI, including the reporting of any breach of protected health information.
- All business associates must enter into an agreement with UPMC to safeguard PHI.
- For more details about these terms and conditions, business associates should refer to the Purchasing section of UPMC's public website.

**Use of PHI for Marketing**

Marketing is defined as any type of communication that seeks to convince an individual to use or purchase a product or service. UPMC must request and obtain written authorization from an individual to use or disclose his or her PHI for marketing purposes.
Examples not considered marketing:

- face-to-face communications, such as when pharmaceutical samples are given to a patient during a doctor's office visit
- communicating additional treatment options, care management activities, or alternative care settings.

Use of PHI for Fundraising

Fund raising refers to any activity to raise charitable donations that support research, education, or the advancement of health care activities within UPMC.

- Types of PHI that may be used for fund-raising purposes without obtaining the patient's authorization must be de-identified and include:
  - demographic information that does not identify the patient (age, race, gender, etc.)
  - dates that health care was provided to a patient

- The Notice of Privacy Practices describes how a patient's PHI may be used for fund-raising activities.
- Use of other types of PHI which identifies the patient, requires a separate authorization from the patient.

Use and Disclosure of PHI for Research Purposes Pursuant to the HIPAA Privacy Rule

All research activities must be conducted in accordance with the rules of the Institutional Review Board (IRB).

- Patients must sign a research authorization for their PHI to be used or disclosed.
- De-identified information (as described in the HIPAA Privacy Rule) may be used for research without the patient's authorization.
- UPMC also uses external institutional review boards for clinical trials such as the Independent Investigational Review Board. For a complete list, contact the UPMC Clinical Trials Office.

Accounting of Disclosures of PHI

Accounting of Disclosures (AOD) is a summary of where a patient's PHI was disclosed and includes a list of those people who have received or accessed protected health information.

- Patients have a right to receive an accounting of disclosures and AODs must be maintained for six years.
  - Subject to a schedule established by federal law, UPMC must provide an accounting of disclosures of all individuals who have received or accessed a
patient’s electronic record for a period of three years prior to the date on which the accounting is requested.

○ In addition, business associates will also be required to supply an accounting of disclosures when requested.

Filing a Complaint - Complaint Management Process

Patients and staff have a right to file a complaint if they feel their privacy rights have been violated. There are many options for filing a complaint.

Staff can file a complaint by first contacting their manager or supervisor. If they are unable to or uncomfortable with doing so, then complaints can be filed by using the same methods available to patients as described below.

Patients (or parent/guardian/other authorized person) can file a complaint by:

● Informing a UPMC employee
● Employee receiving a complaint must report it to the entity privacy
● contacting the entity's privacy officer
● Calling the:

  ○ HIPAA Helpline - 412-647-5757
  ○ Compliance Helpline - 1-877-983-8442 (anonymous option)
  ○ Writing (paper or electronic) to the:

    Secretary of the United States Department of Health and Human Services, 200 Independence Ave, SW Washington, DC 20201.

Patient Access to PHI

Patients have a right to access and review their PHI. A patient must submit a written request and schedule an appointment at the facility where the treatment was provided in order to access his or her PHI.

UPMC may deny a patient access under certain situations:

● contains psychotherapy notes
● compiled for court proceedings
● physician determines not appropriate
● could result in danger to another person
● prohibited by law
**Employees Accessing PHI**

If an employee has an account for a UPMC clinical system, the employee is generally permitted to access the employee's medical information on that system. The exceptions are that (a) an employee is not entitled to access his/her behavioral health or drug/alcohol treatment information; (b) UPMC reserves that right to limit an employee's access to his/her medical information on UPMC Clinical Systems; and (c) an employee's use of UPMC clinical system must not interfere with the employee's or other staff's work.

- Employees are prohibited from accessing medical records of their spouses, children, relatives, and others.
- Employees are permitted only to access information needed to perform their job.
- Employees will be subject to disciplinary action if PHI has been accessed inappropriately and may be subject to fine, imprisonment and termination.

**Patient Amendment to PHI**

Patients may request to amend or correct their PHI, if they feel that UPMC has recorded incorrect or incomplete information about them. A patient who wants to amend his or her PHI must make a written request to the facility holding this where the medical information was created. The request must include the reason the information should be amended.

UPMC may deny a request when:

- request to amend is not in writing
- patient does not include a reason to support the request
- information was not created by the facility
- health care provider verifies the existing information is true and accurate
- facility must notify the patient in writing whether the request to amend was approved or denied
- the patient may submit a statement of disagreement which will become part of the patient record when an amendment request is denied.

**Minimum Necessary Standards for Using PHI**

Protected health information (PHI) is available to UPMC staff on a need-to-know basis. Need-to-know means that you rely on or need PHI in order to do your job.

- However, you should access only the minimum amount of information that you need to perform your job.
- For example, all of the patient's health information is available for a physician, nurse, or other staff member to use to provide direct patient care. However, this same information is not available to the hospital's telephone operator. The need-
to-know information the telephone operator requires is the patient's name and room number.

- Accessing patient information that is not relevant to your job may result in disciplinary action, up to, and including termination.
- A log of all users accessing PHI via electronic means is available to monitor this.

If you are required to disclose PHI to someone for purposes other than treatment, payment or operations, such as a court order, you must verify:

- who the requesting party is
- that they have a need-to-know this information
- that only the minimum necessary information is provided

- If a patient pays for services out of pocket in full, and supplies in writing their request that we do not share this information we are not to release this information.
- Questions regarding the minimum necessary standards for using or disclosing PHI should be directed to your privacy officer or Health Information Management (medical records) department.

**Reporting of Suspected Problems**

It is every employee's responsibility to be alert to unethical behavior or possible violations of UPMC policies.

There are many examples of inappropriate use or disclosure of protected health information.

**These include but are not limited to:**

- Faxing - If the patient's information is sent to the wrong fax number or wrong location, the doctor's office or requesting agent must report this to either HIM or their Privacy officer.
- Patient Identification - If a patient presents with identification that does not appear to be consistent with existing information, contact your privacy officer to notify him or her of the possibility of identity theft.
- Access/Disclosure - All inappropriate PHI access or suspected breach in security shall be reported in accordance with appropriate UPMC Policies.

Communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager if you need assistance. If you are not comfortable or unable to follow the chain of command, the following additional resources are available:
• privacy officer
• compliance officer
• Corporate Compliance Office
• Human Resource
• Legal
• UPMC Compliance Helpline toll-free at 1-877-983-8442 (anonymous)

UPMC prohibits retaliation against anyone for raising, in good faith, a concern or question about inappropriate or illegal behavior. Retaliation is not allowed against anyone participating in an investigation or providing information related to an alleged violation.

Red Flag Rules”: Reporting Suspected Identity Theft

Congress enacted the Fair and Accurate Credit Transaction Act (FACTA) of 2003 which amended the Fair Credit Reporting Act (FCRA) in response to the increase in identity theft. Subsequently, the Federal Trade Commission (FTC) issued the “Red Flag Rules”.

The Red Flag Rules aim to protect the consumer from identity theft. This rule requires that any business entity (“creditors”) who maintain an account (“covered account”) which allows deferred payment and or credit to a client must implement a program to identify, detect, and respond to identity theft.

Identity theft occurs when someone uses another person’s personal information to fraudulently obtain medical services (e.g. name, address, Social Security number, credit card number insurance information or other identifying personal information).

Red Flags are defined as any pattern, practice, or specific activity that could indicate identity theft.

• If you suspect that identity theft has occurred communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager or supervisor who will perform an initial investigation. If you are not comfortable or unable to follow the chain of command, additional resources are available:
  • privacy officer
  • compliance officer
  • UPMC Compliance Helpline toll-free at 1-877-983-8442 (anonymous)
Theft and/or Breach of Personal Information

In General:

A breach occurs when there is an unauthorized acquisition, access, use, or disclosure of protected health information. If you suspect that a breach has occurred, you should notify your supervisor or entity Privacy Officer immediately. If it is determined that there was a breach, UPMC will need to report the breach, including providing written notification to the affected patient(s).

- **Example:** Without a work related need, a nurse intentionally opens her co-worker's record.

- **Exceptions:** There are a variety of exceptions where a breach does not need to be reported, including situations, where it is unlikely that the information could be misused. However, this decision may only be made following an investigation by UPMC.
PATIENT RIGHTS & ORGANIZATIONAL ETHICS

BEHAVIORAL OBJECTIVES:
After reviewing this material the reader will be able to:

- Understand the rights and responsibilities of patients.
- Define Ethics and ethical dilemmas in the organizational setting.
- Identify major areas of ethical dilemmas in an organization.
- Recognize how rights of patients are protected by ethical decision making.

Active participation in care decisions is not a patient’s privilege it is a fundamental right. If however, patients are not given the information needed to evaluate their options, they cannot exercise this right.

As healthcare givers, we must understand these rights so that all activities involving the patient are conducted with concern for him/her, and above all, the recognition of his/her dignity as a human being. Standards have been set which promote consideration and respect of individual values and preferences and includes the decision to discontinue treatment. Important activities related to these standards include advising patients of their responsibilities in the care process and making sure they fully understand the benefits and risks associated with planned procedures.

All hospital employees and medical staff are responsible for ensuring that the patient, parent and/or guardian are involved in all aspects of care. Patients must be involved in at least the following areas:

- making care decisions; giving informed consent;
- resolving dilemmas about care decisions;
- formulating advance directives;
- withholding resuscitative services;
- forgoing or withdrawing life-sustaining treatment and planning care at the end of life.

Standards also recommend that the family be allowed to participate in care decisions, while recognizing the patient’s right to exclude any or all family members. Sometimes it is mandatory that people other than or in addition to the patient be involved in decision-making. This is especially true in the case of un-emancipated minors, when the family or guardian is legally responsible for approving care. Often a surrogate decision-maker must be identified in the event that the patient lacks the mental or physical capacity to make decisions or communicate them.

Ethical decisions regarding care can present all sorts of difficult questions and conflicts for the organization, patients, family members and other decision-makers. Defining ethics and understanding the areas of ethical dilemmas can help us make choices that have a positive impact on individuals and groups involved with the organization.

Ethics deals with right and wrong in the values and actions of individuals and the communities and organizations that they are a part of. Many ethical issues involve factors that make the choice of “right” and “wrong” decisions less than clear. These are called ethical dilemmas.
There are three (3) major areas where ethical dilemmas may occur within an organization. They include: 1) managing human resources; 2) managing stakeholders (customers, shareholders, suppliers, 3) government agencies, accrediting agencies, etc.); and managing one’s own personal career in relation to organizational loyalty.

Ethical decision-making is extremely complex and should be the result of sound reasoning. Four questions should be asked and evaluated thoroughly to help guide a person to an ethical decision. FIRST – consider who is affected by the decision. The more specific you can be about individuals and groups who may experience benefits or costs from a particular decision, the more likely it is that ethical decisions will be made. SECOND – what are the benefits and costs to these individuals or groups? Answering this question requires determining the interests and values of the specific individuals or groups. THIRD – who has rights, or who is entitled to the benefits of the decision? FOURTH – what are the decision rules? Is there government or accrediting agencies that have certain laws, rules or guidelines that must be taken into consideration when making decisions? Certainly, however, ethical decision-making goes beyond laws.

Dealing appropriately with ethical issues and educating patients and their families about their rights are empowering practices. The hospital’s efforts in these areas foster patient’s dignity, autonomy, and positive self-regard. Through education and consideration of ethical issues, patients are made aware of resources, environmental demands, individual strengths and weaknesses, and what they can expect from their on-going relationship with staff and the organization as a whole.

UPMC Horizon has developed a policy that specifically identifies the rights and responsibilities of its patients. A copy of this policy (included in the learning package) is offered to all patients in the form of a PE (patient education) pamphlet. When the patient is incapacitated, the responsible party receives the information. Simply giving the patients a list of their rights, however, is not enough. Instruction should be personal and interactive.

Likewise, a “Code of Ethical Behavior” has also been developed. The policy states that “...no patient will be denied admission to the hospital based on his/her ability to pay; billing statements will be provided for the time frame of service, with any billing complaints addressed immediately; patient confidentiality will be maintained; there will be full disclosure of conflicts of interest for decision makers at all levels of the organization; marketing of UPMC Horizon services or educational programs will not mislead the customer; contractual arrangement with other healthcare providers, educational institutions and payers will define each party’s responsibility; respect for the patient and family in all areas of care will be maintained; patients will be transferred to other institutions which can provide appropriate care when UPMC Horizon cannot; and UPMC Horizon staff and physicians will report all cases of abuse or suspected abuse in accordance with the laws.
INFECTION CONTROL

INTRODUCTION / VALUE STATEMENT:
As an employee of UPMC Horizon, you may be exposed to various microorganisms that can lead to infection. To help reduce the risks of infections for both the healthcare worker and the patient, the Occupational Safety and Health Administration (OSHA) requires employers to provide training in infection control. This packet is designed to protect all employees against the spread of infections.

BEHAVIORAL OBJECTIVES:
After completing his packet, you will know the following:
✓ How to outline the chain of infection.
✓ Good handwashing technique.
✓ The differences among cleaning, disinfecting and sterilization.
✓ How to describe proper measures to handle body secretions.
✓ The immunizations required by staff and patients.

ISOLATION CONTROL INSERVICE
OBJECTIVES:
At the completion of this lesson the learners should be able to:
• Trace changes in the development of isolation practices.
• Describe standard precautions.
• List special measures that must be taken for transmission-based precautions.

OUTLINE:
Development of isolation practices
• Transition from segregating infected person to treating all people as potentially, infectious regardless of known status.

STANDARD PRECAUTIONS:
Replaces former universal precautions and body substance isolation.
• Used for all patients regardless if they are known to have infection or not, applies to handling of blood, body fluids, secretions, excretions, non-intact skin, and mucous membranes.

TRANSMISSION – BASED PRECAUTIONS
Condenses all former categories of isolation into three categories:
1. Airborne precautions
2. Droplet precautions
3. Contact precautions

Specific measures are used in addition to basic standard precautions.
ISOLATION PRECAUTIONS UPDATE
For well over 100 years, the control of infection by isolation has been a significant concern in health care facilities. When one looks at the development of isolation practices (see Highlights in Development of Isolation Practices at end of packet), one can see that we have gone from segregating all infected persons from uninfected people, to isolating people by organism or disease, to treating all people and their body substances as potentially infectious. As new infectious diseases, such as AIDS, appear and our understanding of how to control methods increases, continued change can be expected. In light of continued change and confusion that health care workers have (e.g., which type of body fluids require precautions, the circumstances in which gowns and gloves are needed, and precautions that are necessary beyond body substances isolation to prevent the spread of infection) the Centers for Disease Control and Prevention (CDC) developed new guidelines for isolation precautions.

TWO LEVELS OF PRECAUTIONS
The revised CDC guidelines contain two tiers or levels of precautions:
1. Standard precautions (replaces the former Universal Precautions and Body Substance Isolation, taking the major features of each).
2. Transmission-based precautions (condenses all former categories of isolation into three sets of precautions: Airborne, Droplet, and Contact).

STANDARD PRECAUTIONS
Standard precautions are used to protect against infection from unknown infected persons. In the past, this protection was obtained by following Universal Precautions that involved protection against blood, body fluid and Body Substance Isolation that focused on the isolation of moist body substances, including urine, feces, sputum, sweat, tears, nasal secretions, and vomitus. Now Standard Precautions replaces Universal Precautions and Body Substances Isolation. Whether or not the patients are known to have infections and regardless of their diagnosis, standard precautions are used and apply to the handling of:
- Blood
- All body fluids, secretions, excretions
- Non-intact skin
- Mucous membranes

The goal of Standard Precautions is to reduce the spread of infection by treating blood and body fluids of all patients as though they were infected.

The terms isolation and infection precautions are sometimes used interchangeably, but they are two different practices. Isolation refers to segregating the person who is infected from uninfected persons while infection precautions are the special actions taken to prevent contact with infection-causing organisms. With isolation precautions, the organism is isolated, not the person.
THE SPREAD OF INFECTION
Disease-causing organisms can be transmitted in a variety of ways. The five (5) main routes of transmission are:

1. **Contact**: This is the most common way that nosocomial (facility-acquired) infections spread. Transmission can occur by direct contact which involves contact between the infected person and one who is susceptible or indirect contact that entails a susceptible person touching an object that has been contaminated by an infectious person.

2. **Droplet**: Transmission occurs when droplets from the infected person come in contact with the conjunctiva, oral or nasal cavity. This can occur during talking, sneezing or coughing.

3. **Airborne**: Small droplets are expelled from the infected person and remain in the air or on dust particles for a period of time, to later be inhaled by a susceptible person.

4. **Common Vehicle**: The microorganism is carried by contaminated food, water, or equipment.

5. **Vector borne**: This refers to the spread of infection by vectors such as mosquitoes, flies, and rodents.

The components of Standard Precautions, used in the care of all patients, are as follows:

**Handwashing**
Wash hands after touching blood, body fluids, excretions, secretions, and contaminated items. If gloves are worn, wash hands immediately after removing them. Wearing gloves does not eliminate the need for handwashing!

**Gloves**
Wear gloves when touching mucous membranes, non-intact skin, blood, body fluids, secretions, excretions, and contaminated items. Wash your hands after removing gloves.

**Masks, Eye Protection Face Shields**
Wear a mask, face shield, and eye protection when performing procedures and care activities that are likely to generate splashes of blood, body fluids, secretions, and excretions.

**Gowns**
A gown is to be worn when performing procedures and care activities that are likely to generate splashes of blood, body fluids, secretions, and excretions. The soiled gown is to be removed as soon as possible and hands are to be washed after the gown’s removal.

**Equipment**
Equipment that has been soiled with blood, body fluids, secretions, or excretions should be handled in a manner that prevents contact with skin, mucous membrane, clothing, or
equipment that is to be used with another patient. Follow the facility procedure for the proper discarding of disposable supplies.

Use mouthpieces or other ventilation devices for mouth-to-mouth resuscitation. Place used disposable needles, syringes, scalpel blades, and other sharp objects in a puncture-resistant container.

**Linen**

Linen that has been soiled with blood, body fluids, secretions, and excretions should not come in contact with the skin, mucous membrane, clothing, or equipment of other people.

**Patient Placement**

Patients who contaminate the environment with their blood, body fluids, secretions, or excretions (such as a patient with dementia who expectorates or plays with feces) should be placed in a private room if possible. If this is not possible, discuss infection control measures with Infection Control or Department manager.

**Education**

In addition to all the employees of the facility, patients and visitors should be educated regarding infection control measures through formal classes, informal discussion, poster, and the distribution of printed information.

**TRANSMISSION-BASED PRECAUTIONS**

Special measures must be taken to prevent the spread of infection when a patient is known to be or carries a high risk of being infected. In the past, a variety of isolation precautions were followed to control the spread of infection under the categories of Strict Isolation, Contact Isolation, Respiratory Isolation, TB Isolation, Enteric Precautions, Drainage/Secretion Precautions. **All of these categories are now condensed into three sets of precautions: Airborne Precautions, Droplet Precautions, and Contact Precautions.** The Transmission-Based Precautions are added to the Standard Precautions; in other words, **standard precautions are essential to follow in the care of all patients.**

**Airborne Precautions**

These precautions are aimed toward reducing the spread of both airborne droplet nuclei (particles, 5 microns or smaller that remain suspended in the air for a long period of time) and dust particles that contain the infectious agent. Microorganisms carried in this way can be carried over a considerable distance from the infected patient where they originated. Tuberculosis, measles, and varicella are the types of diseases that can be spread through the airborne route. Precautions for this patient include a private room, limited movement and travel of the patient when transporting, having those who have contact with the patient follow respiratory protection practices (regardless of how brief the contact is!), exhausting room air to the outside, and having negative air pressure and a minimum of six air exchanges per hour in the room.
**Droplet Precautions**
These precautions are intended to reduce the spread of infections carried by droplets five microns or larger from an infected person to a susceptible person’s mouth, nasal mucosa, or conjunctivae. The large droplets can be expelled during coughing, sneezing, and respiratory procedures such as suctioning. Diseases spread through droplets include influenza and mycoplasma pneumonia. It is suggested that a private room be used by a patient who is on Droplet Precautions, however, if this is not possible, the patient can share a room with a patient with the same type of infection or one who is low risk. (A low risk patient is one who is not confused, has no wounds, and no invasive devices.) Other precautions include the use of a mask when entering the room or within three feet of a patient and having the patient wear a mask when transporting.

**Contact Precautions**
Contact precautions are taken to reduce the spread of infection through:

- **Direct Contact**
  1. Skin of infected person
  2. Skin of susceptible person

- **Indirect Contact**
  1. Inanimate objects, i.e., bedside commode, bed rails, IV poles

Scabies, clostridium difficile, and multidrug resistant organisms are causes for contact precautions to be used.

Contact precautions include the use of a private room or shared room with a patient who is low risk or who has a similar infection, equipment dedicated solely for the patient’s use, and protecting the removal of infected material.

These precautions are summarized on the following pages.
<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>STANDARD PRECAUTION</th>
<th>AIRBORNE PRECAUTIONS</th>
<th>DROPLET PRECAUTIONS</th>
<th>CONTACT PRECAUTIONS</th>
</tr>
</thead>
</table>

**TRANSMISSION-BASED PRECAUTIONS**

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>STANDARD PRECAUTION</th>
<th>AIRBORNE PRECAUTIONS</th>
<th>DROPLET PRECAUTIONS</th>
<th>CONTACT PRECAUTIONS</th>
</tr>
</thead>
</table>

**DESCRIPTION**
- Reduces the risk of spreading infection by the blood, body fluids, secretions, and excretions of all patients as though they were infected regardless if the patients are known to be carrying infection or not.
  - Reduces the risk of spreading infectious agents that can be carried in the air by droplets (small particles 5 microns or less) or on dust particles, and inhaled by susceptible patients.
  - Reduces the risk of spreading infectious agents that can be transmitted by the infected persontouching a susceptible person (direct contact) or by the infected person touching an item or surface that is then touched by susceptible person (indirect contact).

**EXAMPLES/DISEASES**
- Applies to all patients.
  - Measles, varicella, (chickenpox, herpes, zoster or shingles), tuberculosis.
  - Pneumonia, influenza, meningitis, sepsis, streptococcal infections, mumps, rubella, pertussis.
  - Herpes simplex (fever blister), impetigo, pediculosis, scabies, conjunctivitis, multidrug-resistant bacterial infections, hepatitis, and infections caused by shingle, clostridium difficile, or escherichia coli.

**HAND-WASHING**
- After touching blood, body fluids, secretions, and contaminated items.
  - After removal of gloves.

**ROOM PLACEMENT**
- No special precautions unless patient is at risk for contaminating the environment with blood, body fluids, secretions, and excretions, then private room is recommended. Consult with Infection Control if a private room is unavailable for this patient.
  - Private room that has monitored negative air pressure in relation to surrounding areas, at least six air changes per hour, and discharge of room air to outdoors or special filtration system. Keep room door closed. If private room is unavailable, place patient in room with a patient who has similar infection.
  - Private room. If private room is unavailable, place in room with patient with similar infection or with low risk roommate (i.e., one who is not confused, has no open wounds, and no invasive devices). Maintain at least three feet of separation between infected patient and other patients and visitors.
  - Private room. If private room is unavailable, place in room with patient with similar infection or with low risk roommate (i.e., one who is not confused, has no open wounds, and no invasive devices).

**GLOVES**
- When touching mucous membranes, non-intact skin, blood, body fluids, secretions, excretions, and contaminated items.
  - When entering patient’s room and having contact with patient and infective material.
<table>
<thead>
<tr>
<th><strong>TRANSMISSION-BASED PRECAUTIONS</strong></th>
<th><strong>STANDARD PRECAUTION</strong></th>
<th><strong>AIRBORNE PRECAUTIONS</strong></th>
<th><strong>DROPLET PRECAUTIONS</strong></th>
<th><strong>CONTACT PRECAUTIONS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mask, Eye Protection, Face Shield</strong></td>
<td>During procedures when there is likelihood of splashing or spraying blood, body fluids, secretions, or excretions.</td>
<td>Wear respiratory protection when entering room of patient with known or suspected infectious tuberculosis. Avoid entering room of patient with known or suspected measles or varicella if susceptible to these infections.</td>
<td>Wear a mask when working within three feet of patient.</td>
<td>During procedures when there is likelihood of splashing or spraying blood, body fluids, secretions, or excretions.</td>
</tr>
<tr>
<td><strong>Gown</strong></td>
<td>During procedures when there is likelihood of splashing or spraying blood, body fluids, secretions, excretions, or when soiling of clothing is likely.</td>
<td>During procedures when there is likelihood of splashing or spraying blood, body fluids, secretions, excretions, or when soiling of clothing is likely.</td>
<td>During procedures when there is likelihood of splashing or spraying blood, body fluids, secretions, excretions, or when soiling of clothing is likely.</td>
<td>Same as standard precautions. Whenever entering the patient’s room if contact with the patient or the patient’s equipment is expected or when resident has diarrhea, ileostomy, colostomy, drainage, or incontinence.</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td>Handle with caution and clean before use with other patient if soiled with blood, body fluids, secretions, or excretions.</td>
<td>Handle with caution and clean before use with other patients if soiled with blood, body fluids, secretions, or excretions.</td>
<td>Handle with caution and clean before use with other patients if soiled with blood, body fluids, secretions or excretions.</td>
<td>Dedicated for use of patient. If equipment must be shared assure adequate cleaning and disinfection between use.</td>
</tr>
<tr>
<td><strong>Linen</strong></td>
<td>If soiled with blood, body fluids, secretions, or excretions, hand, transport, and process in a manner to prevent exposure to skin and mucous membranes, and avoid contamination of clothing.</td>
<td>If soiled with blood, body fluids, secretions, or excretions, handle, transport, and process in a manner to prevent exposure to skin and mucous membranes, and avoid contamination of clothing.</td>
<td>If soiled with blood, body fluids, secretions or excretions, handle, transport, and process in a manner to prevent exposure to skin and mucous membranes, and avoid contamination of clothing.</td>
<td>If soiled with blood, body fluids, secretions, or excretions, handle, transport, and process in a manner to prevent exposure to skin and mucous membranes, and avoid contamination of clothing.</td>
</tr>
</tbody>
</table>
Once you have read the packet entirely, please complete the bottom of this form and return to the Education Services Department.

As a UPMC Horizon Job Shadow Candidate, I understand that I have to complete the job shadow form and comply with ALL UPMC Hospital Policies.

By signing below, I acknowledge that I have read, reviewed, and understand the Job Shadow Orientation packet that was provided to me.

All questions/concerns that I had have been answered clearly and I know that ALL UPMC Policies can be found on the INFONET should I need to reference the information.

Name(print)______________________________

Signature______________________________

Date: _____/ ____/ _________