



To: All Job Shadowing Students
From: Donna Hopkins – Foundation / Volunteer Manager
RE: Job Shadow Application Packet and Safety Training

All Job Shadow Students need to complete the following:

1) Job Shadow Application Packet

2) Safety Training Packet:

Safety Codes (packet)

HIPAA (Health Insurance Portability and Accountability Act of 1996)

Training (packet)

Confidentiality Training

Abuse/Neglect Training

To complete the Job Shadow Application Packet fill out both sides of the forms. Make sure every blank is filled in with the right information.

To complete the Safety Training Packets you will need to read the information sheets or booklets, and packet, then fill in the test & sign with the correct date. It is not cheating to look at the information sheets or the information booklets when answering the questions on the tests. Looking back at the information to answer questions is part of the training process.

After you have completed the Job Shadow Packet & the Safety Training Packets, please schedule an appointment by calling 546-2301. All the paperwork has to be reviewed by me, before you start your job shadowing experience.

Thank you for taking the time to complete these packets.

A handwritten signature in blue ink that reads "Donna Hopkins".

Donna Hopkins

STUDENT SHADOWING EXPERIENCE AGREEMENT

This agreement is made and entered by and between _____ and
Lourdes Medical Center on the _____ day of _____.

1. The school or organization will supply a list of students cleared for shadowing to the Director of Volunteers at least one week before shadowing.
2. Students will be required to complete a Student Shadowing Packet before arriving at the facility.
3. The packet will require the student to sign a confidentiality agreement, parent permission form, familiarize him or herself with safety code information sheet and comply with dress code before reporting to their assigned clinical department.
4. In accordance with the Facility policy, the Student/Parents are required to have medical coverage in case of emergency treatment of injury or illness occurs while at the Facility.
5. Student will not be allowed to have physical contact with patient. Student will not be allowed into patient room during exam or acute procedure or at anytime without written permission from patient. Failure to adhere to the above mentioned will constitute a breach of patient rights.

School/Organization

Teacher _____

School _____

Phone# _____

Address _____

City & State _____

Student

Name _____

Date of Birth _____

Phone # _____

Address _____

City & State _____

Parent (if student is under 18 yrs)

Name _____

Signature _____

Phone# _____

Address _____

City & State _____

Lourdes Staff

Name _____

Signature _____

Phone# _____

Address _____

City & State _____

Volunteer/Student Oath

I _____, to here by promise to uphold Lourdes Health Networks Mission & Beliefs as follows:

Mission

Our mission is an extension of the healing ministry of Jesus. We are called to serve our community, our patients, their loved ones, and our co-workers with respect, compassion, and care. We respond to the health care needs of the community in a Christian spirit. We strive for excellence in all we do.

Beliefs

- Health care is a human service that fosters healing and wellness on many levels.
- The patient is at the center of our service.
- We promote an environment of mutual respect, creativity and teamwork among our employees, volunteers and medical staff.
- Innovation, creativity, flexibility and excellence are essential in responding to the changing health care environment.
- Good stewardship must be a way of life; our service must be high quality and cost effective, delivered in the context of sound business practice.
- We maintain a close relationship with our community.

Our Call to Action is:

- Healthcare that works.
- Healthcare that is safe.
- Healthcare that leaves no one behind.

Print name

Date

Signature

Witness

Student Job Shadow Experience Verifications

Date : _____

Student Name: _____

Student School: _____

School Contact Name & phone #: _____

Lourdes Employee to be shadowed: _____

Lourdes Employee name

Lourdes Department

Phone extension _____

Starting Date: _____ Ending Date: _____

<u>Requirement</u>	<u>Date</u>	<u>Initials</u>
<input type="checkbox"/> Confidentiality Agreement	_____	_____
<input type="checkbox"/> HIPAA Training	_____	_____
<input type="checkbox"/> Completion of Safety Training	_____	_____
<input type="checkbox"/> Age & Cultural Competencies	_____	_____
<input type="checkbox"/> Volunteer/Student Agreement	_____	_____
<input type="checkbox"/> Student Name Tag	_____	_____
<input type="checkbox"/> Dress Code	_____	_____



LOURDES HEALTH NETWORK NEW EMPLOYEE SAFETY EDUCATION

1. Please review the contents of this packet.
2. Complete the New Employee Safety Education Form. (enclosed)
3. Have Volunteer Manager sign to confirm that you have received and read this training packet.
4. Keep the Safety Packet for your future use.

THIS SAFETY PACKET MUST BE COMPLETED ON THE FIRST DAY OF EMPLOYMENT



FIRE SAFETY

Responding to a fire: CODE RED

R.A.C.E. = Rescue, Activate, Contain, Evacuate

Rescue anyone in danger

Activate fire alarm

Pull the nearest fire alarm pull station

Call the operator using the emergency number

(330 at Lourdes Medical Center(LMC) and report the exact location of fire)

(0 at Lourdes Counseling Center(LCC) and report the exact location of fire)

Contain the fire

Close doors and windows

See that fire doors are closed

Evacuate the building – or –

Extinguish the fire if it safe to do so

Use the nearest fire extinguisher or smother the fire

(At LMC relocate if indicated. Move the occupants to a safe area; <other side of fire door>, clear hallways of obstacles)

How to use a fire extinguisher:

P.A.S.S. = Pull, Aim, Squeeze, Sweep

1. Hold the extinguisher upright and **PULL** the ring pin, snapping the plastic seal.
2. Stand back from the fire, **AIM** at the base of the fire.
3. Keeping the extinguisher upright, **SQUEEZE** the handles together to discharge.
4. **SWEEP** from side to side.
5. When fire is out, watch for re-ignition.
6. Evacuate and ventilate the area immediately after extinguisher use.



ELECTRICAL SAFETY

1. Do not overload electrical circuits
2. Check electrical cords for wear, loose plugs or prongs and missing ground plugs
3. Grab the plug when unplugging electrical equipment, not the cord.
4. Do not put electrical cords where they can be stepped on or tripped over.
5. Report any potential electrical hazard to your instructor or supervisor
6. Electrical equipment or devices must be checked by maintenance prior to initial use.
7. **At LMC, red receptacle covers designate emergency outlets with backup generation**



M.S.D.S

A Material Safety Data Sheet (MSDS) gives a person detailed information on a specific product and its potential hazards. All departments within the health center will contain the MSDS information specific to that department.

The MSDS will list the following information about a potentially hazardous product:

1. Product name
2. Chemical type
3. Formula
4. Trade name
5. Special protection information
6. Appearance/odor
7. Special precautions and spill/leak procedures
8. Hazardous ingredients
9. Physical and chemical characteristics
10. Physical hazards
11. Health hazards
12. Emergency and first aid procedures



SAFE MEDICAL DEVICE ACT

What is a medical device?
How must we comply?

Any equipment or product used in the care of patients.
The hospital must report occurrences which cause serious illness or injury, defined as:

- Life threatening.

- Results in permanent impairment of a body structure or function.
- Needs medical or surgical intervention to prevent permanent damage to a patient.

When must the occurrence be reported to the FDA?

Within 10 working days after the occurrence.



BODY MECHANICS – Injury Prevention

Principles: Maintain normal curvature of the spine
Shorten the lever arm
Use the strong back and leg muscles

Techniques:	Size up the load	Pivot your feet	No jerking movements
	Bend the knees	Don't twist your back	Break up large loads
	Keep wide base of support	Face the object squarely	Communicate to your partner
	Tighten abdominal muscles	Lift with your legs	Get Help
	Plan ahead	Keep load close to your body	

STOP AND THINK



BODY SUBSTANCE PRECAUTIONS

1. Body Substance Precautions

- a. Unable to tell for sure which patients carry any blood borne pathogen
- b. HIV and HBV infect people of all ages and background
- c. The patient may not know they are infected.
- d. All patients must be treated as if infected
- e. All body fluids are potentially infective

2. Reducing your risk – five major ways

- a. None are 100%
- b. Must use these five ways together
 - (1) Engineering controls – patient environment
 - (2) Safe work practices
 - (3) Personal protective equipment
 - (4) Housekeeping – clean up after yourself
 - (5) Hepatitis B vaccination

3. Engineering controls physical or mechanical systems to eliminate hazards

- a. Self sheathing needles
- b. Needle boxes
- c. Needle less systems
- d. Effectiveness depends on you

4. Work Practice Controls – Specific procedures you follow

- (1) **At LMC: If you see a stop sign on the patient door, report to nurse before entering for special instructions.**
- a. Needle stick prevention
 - (2) Do not bend, hand recap, shear or break needles or sharps
 - (3) **At LMC, recap or remove only when medically necessary**
 - (4) **At LMC, use one-handed technique or mechanical device to recap**
 - (5) Place in sharps container immediately
- b. Hand washing – the sooner the better
 - (1) Hand washing prevents transmission to other areas of the body and other surfaces
 - (2) Hands must be washed every time you remove gloves
 - (3) Flush skin or mucous membranes with water if exposed
- c. Personal Hygiene
 - (1) Minimize splashing, spraying or spattering when possible
 - (2) Do not eat, drink, smoke, apply cosmetics or lip balm or handle contact lenses in work area
 - (3) Avoid petroleum based lubricants – may damage gloves
 - (4) Never mouth pipette or suction blood or other materials
 - (5) Never keep food or drinks where they may be contaminated

5. Personal Protective Equipment (PPE)

- a. Equipment that protects you from contact with potentially infectious materials:
 - (1) Examples: gloves, mask, gown, apron, lab coat, face shield, protective eye wear, mouthpiece, resuscitation device
 - (2) Hazard: Generation of splashes, sprays, spatter or droplets
 - (3) Protection: mask, gloves, eye protection, gown, face shield
 - (4) Hazard: Potential clothing or skin exposure
 - (5) Protection: gown, gloves, apron, and other protective body clothing
 - (6) Hazard: encountering large amounts of blood during surgery or autopsy
 - (7) Protection: gloves, gown, surgical cap/hood, shoe covers/boots
- b. General Rules on PPE
 - (1) You should be trained in its use by your instructor or supervisor
 - (2) It must be appropriate for the task
 - (3) You must use appropriate PPE each time you perform the task
 - (4) Your PPE must be in good condition
 - (5) Your gloves must fit properly
 - (6) If PPE is penetrated by blood, remove it as soon as possible
 - (7) Remove all PPE before leaving work area
- c. Exceptions to the rule
 - (1) If you believe that PPE will prevent proper delivery of health care or jeopardize your safety or a co-worker's safety, you may temporarily and briefly abandon its use in an emergency.
 - (2) After the incident, the health center must investigate the circumstances to determine if such a situation could be prevented in the future
 - (3) In ALL other situations, PPE is mandatory.
- d. Avoid unprotected mouth to mouth resuscitation
- e. Gloves are the most widely used PPE
 - (1) Must wear gloves when you anticipate hand contact with blood or body fluids
 - (2) If allergic, hypoallergenic gloves will be provide
 - (3) Bandage cuts prior to wearing gloves
 - (4) Replace gloves as soon as possible after contamination
 - (5) Never wash gloves for reuse
 - (6) Use gloves carefully to avoid contamination

6. Housekeeping

- a. Good housekeeping protects every healthcare worker
- b. This is everyone's Responsibility
- c. General Rules
 - (1) Clean and decontaminate at the end of each work shift
 - (2) Clean as soon as possible after contact with blood or body fluids
 - (3) Do not use hand to pick up broken glass which may be contaminated
 - (4) Handle contaminated laundry as little as possible, place in proper container
 - (5) Pay attention to bio hazard labels

7. HBV vaccination

- a. The vaccination is a synthetic product and is not infective
- b. It is 85-95% effective at protecting you from HBV
- c. Requirements for HBV vaccination are student contract specific
- d. Exposure
 - (1) If you are exposed, report the incident immediately to your instructor or supervisor.
 - (2) Each health center has an exposure plan
 - (3) If you have questions or concerns about protection from exposure, talk with your instructor, supervisor, or the infection control practitioner at the health center.



HOSPITAL SPECIFIC SAFETY EDUCATION

1. Disposal of Hospital Waste

- a. Body substances from all patients are considered potentially infectious.
- b. Trash and disposable items soiled with body substances are placed in clear plastic bags to prevent leakage
- c. (At Lourdes Medical Center, items that can be emptied (suction canisters, drainage bags, etc.) will be carefully flushed into the sewer system prior to disposal. Isolyzer will be used in the OR for collection systems which are difficult to empty or contain a large volume of blood/body substance.)

2. Dressing and Other Solid Waste

- d. Any dressing materials that could potentially release blood or body fluid are disposed of as bio hazardous waste.
- e. These items are placed in a red bag and disposed of in a trash receptacle in the dirty utility room

3. Needles and Other Sharps

- f. Disposal of needles and other sharps is the responsibility of the person using the item.
- g. Sharps containers are located in all patient care areas
- h. (At Lourdes Medical Center, sharps containers are also available in all of the IV trays.)
- i. Never overfill a needle box.
- j. These are checked daily by housekeeping personnel for replacement, but may be replaced by whomever finds the container full.

4. Linens

- a. All linens are to be treated as contaminated.
- b. (At Lourdes Medical Center, linen is to be placed into the that is located in the nurse server.)
- c. Linen is never to be placed in red trash liners. Anything placed in a red container or liner is incinerated.



LMC – COMMON CODES

List of Common Codes

For any questions contact patient Care Supervisor, beeper number 545-7917, or the department manger.

1. **CODE RED: Fire Emergency**
 - a. Begin **R-A-C-E** steps:
 - (1) **R**=Rescue – remove anyone in immediate danger from fire or smoke
 - (2) **A**=Activate the Alarm – pull the nearest alarm
 - (3) **C**=Close all doors and windows tightly
 - (4) **E**=Evacuate – follow evacuation procedures
 - i. Extinguish – use fire extinguisher **ONLY** if fire is small and can easily be extinguished
2. **Code Grey: Combative Person**
 - a. Use whenever it appears that physical restraint may be necessary.
 - b. **Dial 330** to reach Operator and report location of incident or where assistance is needed.
 - c. All of the Maintenance/Security, House Supervisor and male employees should respond.
3. **Amber Alert: Child Abduction**
 - a. Use when discovering a child or baby missing
 - b. Immediately call Operator (**Dial 330**) and state “Code Pink on _____(Dept)”. Operator will alert PD.
 - c. Notifies Primary Resource Nurse (Charge Nurse) who will question parents, visitors, etc.
 - d. Quietly alert other staff in the department who will conduct a search of entire unit.
 - e. An accounting of all infants is made.
4. **Code Yellow Class (A or B) Disaster Plan**
 - a. The operator will announce the disaster as Code Yellow, class A (=less than 25 casualties) or B (=25 or more casualties).
 - b. Refer to Emergency Plan located in each department for department plan
5. **Trauma Code**
 - a. Used to activate the Trauma Response Team, on order of the Emergency Department Physician
6. **Code Blue**
 - a. Used for cardiac or respiratory emergency
 - b. Push **Blue** code buttons located in most patient rooms or **Dial 330** to contact the operator and report the room number
7. **Remember C-H-E-M: CODE ORANGE**
 - a. **C**=Contain the spill/leak immediately
 - b. **H**=Call for help (**Dial 333** and notify of product and exact location.)
 - (1) Call Department Manager
 - (2) Operator will notify Emergency Response Team.
 - c. **E**=Evacuate the immediate area
 - d. **M**=Locate the MSDS in each Department’s Right to Know Book located in each department

SAFETY RULES FOR ALL EMPLOYEES, DEPARTMENTS, AND FACILITIES:

The following items are not intended to be a complete list of safety rules or issues for employees, but rather a review of general safety issues. Employees must become familiar with the Policies and Procedures that pertain to their specific department and job duties.

- Parking is limited, follow parking rules
- Keep cars locked, windows up
- Do not keep valuables in cars
- Keep purses out of sight, bring only essentials in your purse
- DO NOT argue with an offender – Call CODE VIOLET at LCC ext. 333 and at LMC ext. 330
- Obey and enforce the NO SMOKING Policy
- Know where fire alarms and extinguishers are located and how to use them
- Know how to operate equipment. Do not use until trained or ask for instructions
- Practice good housekeeping rules. Keep work areas and halls free of clutter, clean up spills immediately
- Remove broken glass at once
- Observe ISOLATION signs and rules
- Walk Don't Run
- Assist a patient or visitor whenever necessary
- Report defective equipment immediately and remove it from the area so it may be repaired or replaced. Beware of electrical services and hazards
- Know all Emergency Plans, Fire, Disaster, Bomb Threat, Hazardous Materials, Security
- Practice good body mechanics. Know and use proper techniques for lifting, reaching, pushing, bending, etc. If an object is over 51 lbs get help.
- Report all incidents, accidents, injuries, or errors that involve patients, visitors, or employees. An Occurrence Report Form must be completed and filed.
- Call Security Officer to walk with you to your car at LMC, or insure you can be observed by co-workers at LCC when going to your car after dark, when working evening or night shift.



LOURDES HEALTH NETWORK
New Employee Safety Education Form

If you have read the Safety Education Packet, Please check off the following:

- Fire Safety**
- Electrical Safety**
- Material Safety Data Sheets**
- Safe Medical Device Act (at Lourdes Medical Center)**
- Body Mechanics Injury Prevention**
- Body Substance Precautions**
- Hospital Specific Safety**
- Common Codes**
- General Safety Rules**

I have completed a review of the above listed safety materials. I understand my responsibilities in response to an emergency. I also understand that I am still expected to complete General Orientation.

(Signature)

(Date)

I have been shown and can recognize the red **Emergency Plan** notebook. I understand that a similar notebook can be found on my department and will be shown to me during orientation to my department.

(Signature)

(Date)

I have been shown and can recognize the light blue **Infection Control Manual**. I understand that a similar notebook can be found on my department and will be shown to me during orientation to my department.

(Signature)

(Date)

I have been shown the online **Personnel Policy Manual**. I understand that I can access this manual from any computer as soon as I have been issued a password. Until such time, personnel policies may be viewed in Human Resources department

(Signature)

(Date)

I have been shown the online **Mandatory Safety Data Sheet (MSDS)**. I understand that I can access this manual from any computer.

(Signature)

(Date)

I hereby verify that this new employee has been provided with the training listed above.

(HR Signature)

(Date)

(Employee's Name)

(Department)

HIPAA TRAINING

Building a Privacy Foundation

The information in this packet will focus on key concepts and terms included in the Health Insurance Portability and Accountability Act (HIPAA) privacy rule and discuss best practices in maintaining the confidentiality of patients' health information.

Setting the Standard for Privacy

We will be covering 6 (six) areas that will help us build a privacy foundation. They are:

1. Health Insurance Portability and Accountability Act (HIPAA)
2. Patient Bill of Rights
3. Federal and State Regulations
4. Accreditation Standards
5. Case Law
6. Professional Standards of Practice

HIPAA

Healthcare organizations are governed by a variety of standards and regulations depending on the type of healthcare setting. HIPAA enacted sweeping changes by passing privacy standards that apply to most healthcare organizations around the country.

HIPAA has placed a spotlight on privacy. However, privacy is not a new issue for healthcare. Maintaining the confidentiality of patient information has always been important.

Patient Bill of Rights

The Patient Bill of Rights guarantees confidentiality of an individual's health information.

Federal & State Regulations

Federal and state regulations address confidentiality by requiring applicable organizations to have policies in place to protect the privacy and security of health records from loss, destruction and unauthorized use.

Case Law

Our Country's courts have also played a part by setting guidelines on confidentiality and patient access to their own records through case law.

Professional Standards of Practice

Professional practice standards, such as those established by the American Health Information Management Association, outline the basic standards in protecting confidential information. Health information professionals are bound by a code of ethics that requires them to promote and protect the confidentiality and security of health information and health records.

What Must be Kept Confidential?

The HIPAA rules define the type of information that must be kept private by categorizing it as "Protected Health Information" or PHI for short. Healthcare organizations must have policies in place that maintain the privacy of PHI.

What is PHI?

PHI is any and all information about an individual's physical or mental health that identifies the individual. This includes any type of information found in the medical and billing record, such as a history and physical exam, diagnoses, progress notes, etc.

PHI includes demographic information such as name, address, phone/fax number, email address, date of birth, social security number, names of relatives, photographs and any type of information that could identify the individual.

PHI exists in many forms. Traditionally, policies have been developed to protect written information such as the medical and billing records. There are policies covering security measures for electronic health records and databases. In addition, there are policies that address to written PHI and orally communicated PHI.

As a rule of thumb, private information that you see, hear, or say must be kept in confidence. PHI should only be disclosed for specific purposes related to an individual's treatment, payment for services they received or related to the operations of the healthcare organization.

Use of PHI: Sharing, applications, utilization, examination or analysis of PHI within an organization.

The terms "use" and "disclosure" are important in understanding how to appropriately protect an individual's privacy while completing one's job responsibilities. These terms are used frequently in the HIPAA Privacy Rule and may be referred to often.

The term "use" refers to how confidential PHI is used with in an organization to treat the patient, complete the billing function and support facility operations. You may use PHI in your job by sharing, applying, utilizing, examining or analyzing confidential information.

Disclosure of PHI: When to release, transfer, access or divulge PHI to an outside person or entity.

Disclosure relates to how you communicate PHI to an outside person or entity. Whether the information is released orally, transferred via fax, accessed through the computer system, discretion must be used when disclosing information. The receiving party must be authorized and have a need to know.

Minimum Necessary Access

The type of information you need to access depends on what you "need to know" to do your job. Accessing, using or disclosing PHI on a need to know basis to accomplish your job responsibilities is an important concept under HIPAA. It is referred to as "minimum necessary information".

The HIPAA rule requires an organization to define who has access to PHI and identify what they can and cannot access.

HIPAA requires organizations to do this by:

- **Identify members of the workforce who need access to confidential information.**
- **Identify what information can be accessed.**
- **Limit access when needed.**

How do you know when information is considered private? If you learned of the information through your job, it is considered private.

When you work in a healthcare organization, you are exposed to confidential information all the time. What you do with the information is critical. How do you decide when information is considered private and when it is not?

If you see, hear or read information through your job, it is considered confidential and you must keep it to yourself. Consider this scenario: In doing your job you find out that a friend has come to your facility for treatment. You would like to go see him/her and offer moral support.

Can you do this? No. You learned the information through your job and you should not use it for personal reasons.

What if the sister of your friend calls you and tells you they are at your facility for treatment? You have learned this outside of your job and can go see your friend to offer moral support.

Gaining Access to Personal Medical Records

HIPAA give individuals an array of privacy rights and more control over how their confidential information is used and disclosed. Here are a couple of scenarios you may encounter.

- 1. How do I handle an individual asking for access to their records?**
 - Individuals have the right of access. You need to route the request to the Medical Records Department. They are familiar with the rules and regulations regarding release of information.**
- 2. How do I handle a parent wanting access to their child's records?**
 - Parents have the right to access their children's records with some exceptions. You should refer these requests to the Medical Records Department.**
- 3. How do I handle a spouse wanting access to their partner's records?**
 - You need to refer such requests to the Medical Records Department as they are familiar with the laws governing release of information.**

Changes in an Individual's Medical Records

Individual's have the right to request changes be made to their medical records after they have read it. However, the request will be reviewed or investigated to ensure it is appropriate. When an individual requests an amendment to their PHI, the request should be referred to the Medical Records Department.

Requests for Information About a Patient

If an individual is asking for information about a patient they must know the patient's first and last name. If the patient's first and last name is provided you may give out the patient's room number and the one word condition as long as the patient has agreed to be listed in the hospital directory.

What if a family member or close friend is asking for clinical or billing information?

- Refer the individual to the patient for such information.**
- If the patient is not able to give the information, consider who the person is and their relationship to the individual and disclose only the information that is pertinent to the relationship. For example, if the person requesting the information is a relative and holds a Power of Attorney, it would be appropriate to disclose the information.**

- **Do not disclose information about a patient to friends of the patient. These persons must obtain information from the patient or a Care Partner of the patient. You should not disclose PHI to them.**

What if a co-worker inquires about a patient condition or treatment?

- **Determine if it is necessary to their position. Is the disclosure of PHI necessary for the co-worker to do their job? If so, disclose only the information the employee needs to do their job.**
- **Determine if it is related to the treatment of the patient. If so, disclose only that information that is necessary for treatment of the patient.**

If the patient's PHI is not needed for the person to do their job or for treatment of the patient, the confidential information should not be disclosed to them.

Privacy Friendly Practices

There are everyday things you can do beyond the regulations and standards that will help protect patient privacy.

- **Review the Notice of Privacy Practices given to each individual and abide by the content.**
- **Make sure any documents containing PHI are shredded before throwing them in the garbage. Doing this will help to ensure that the patient's confidential information is not inadvertently seen by unauthorized individuals.**
- **If fax and copy machines are used to send or copy PHI, make sure they are located away from public areas.**
- **Always consider where you are talking about confidential information. Are you in a public area where others can overhear your conversation? Whether you are talking to a patient, family member or other employees, try to keep your conversations from being overheard. If possible move to an unoccupied corner or another room to protect the privacy of PHI.**
- **Keep PHI out of public areas such as waiting rooms, conference rooms, the top of a nursing station or receptionist desk or on white boards viewable by the public.**
- **An important aspect of protecting patients' privacy is keeping their records secure regardless of where they are kept. If a medical record is kept in an office and the office is unattended, how will the record be stored?**
- **Confidential information and records on computers are kept secure through adherence to facility policies such as passwords protection. Passwords should be unique to each member of the workforce and never shared or easily identified.**
- **Computer screens should be turned or positioned to prevent the public from viewing the information. Privacy screens could be placed over the computer screen so that no one but the person sitting in the chair directly in front of the computer can see what is on it.**
- **When providing treatment consider where you are and who is around the patient. Help protect the patient by giving them the opportunity for privacy when providing treatment or discussing their condition.**
- **Recognize the importance of providing quality healthcare with the maximum security of personal healthcare information. It takes all of us to make sure everyone's PHI is secure.**

HIPAA Training TEST

Please circle True or False to each question. You may look back into the information to answer each question if necessary.

1. HIPAA stands for Health Insurance Portability & Accountability Act.

True False

2. Healthcare organizations are governed by a variety of standards and regulations including but not limited to State and Federal guidelines.

True False

3. Employees, volunteers or medical staff do not need to refrain from discussing PHI in waiting areas, lobby areas, hallways or any public areas.

True False

4. A patient does not have the right to request an amendment to his/her medical records.

True False

5. Patient authorizations are required for any use or disclosure of PHI not covered by consent.

True False

6. There are both civil and criminal HIPAA penalties if the regulations are not followed.

True False

7. You should refer any individual requesting a copy of their medical records to the Medical Records Department.

True False

8. Under HIPAA, using PHI for any marketing activities is permitted as long as all identifiable information is taken off the data.

True False

9. If a patient's name is removed from a record, it is no longer considered individually identifiable information that is protected under HIPAA.

True False

10. PHI includes the patient's name, address, phone, fax number, email address, date of birth, social security number, relative names, photographs, and other types of information that could identify the individual.

True False

Signature

Date



Lourdes Health Network

POLICY/PROCEDURE

FACILITY: LHN
 DEPT NO: 01.8650
 POLICY NO: 5300.06
DEPARTMENT: Human Resources
TITLE: Dress Regulations and Appearance

POLICY:

Associates must present a professional, business-like appearance that reflects the proficient care and high standards of Lourdes Health Network. Associates work attire should compliment an environment that reflects an efficient, orderly and professionally operated organization.

Immediate supervisors, department directors and managers must communicate and enforce LHN's dress code and their departmental dress code. Counseling of dress code violators should be a first step, corrective measure. In certain situations, if an associate's attire is judged by a supervisor to be in noncompliance with this policy, he/she may be sent home, on unpaid time. Progressive disciplinary steps may be applied where noncompliance continues, up to and including termination.

This policy applies to LHN associates, contract staff, medical staff employees, volunteers, and students, all shifts, all days of the week, and representing LHN off-site when volunteering at events, such as county fairs, safety fairs, etc. This policy does not necessarily apply to associates who are in the hospital during off duty hours.

PROCEDURE:

DRESS REGULATIONS AND APPEARANCE

1. General Requirements

Good grooming must be maintained at all times.

Basic rules of personal hygiene must be maintained for infection control purposes, to include clean, properly trimmed fingernails and neatly trimmed facial hair, to maintain a proper appearance, and to prevent unpleasant body odors. In patient care areas, hair must be tied back when it is more than shoulder length.

Original Effective Date: 6/1/74

Original Dept.

Human Resources

Supersedes: LMC Pol # 5300.20 11/99

Administration: 6/74; 4/92

LCC Pol # 414.7 11/99

Amburgey & Rubin: 6/04

Infection Control: 6/04

Dates Reviewed: 5/75; 3/77; 4/79; 4/80; 4/81;9/82; 5/83; 11/84;

Dir/Mgrs/Sup: 7/04

12/85; 8/86;8/87;9/89;1/92;3/96;3/98;7/06;6/07;5/08;4/09

Dates Revised: 7/74; 2/82; 11/84; 4/92; 11/99; 7/04

Fingernail length is a clinical and safety issue, for employees and patients. In patient care areas, the standard for fingernail length is 1/4" or less from the end of each finger. Departments may have this standard applied for safety reasons in non-clinical areas. Under the Infection Control policy, artificial fingernails and extenders are prohibited on associates providing direct patient care.

Perfume, cologne, and scented lotions are not acceptable in patient care areas. In non-patient care areas perfume, cologne and scented lotions may be worn in very limited amounts not offensive to others and others allergies. Please be considerate of co-workers, asking if your perfume, cologne, or scented lotion is offensive to them.

Associates having contact with patients and/or machinery are to keep jewelry to a minimum for safety reasons.

Make-up is to be used in moderation.

For safety, footwear must be appropriate for the work area. Staff should avoid wearing leather soled, high heels, open-toed, "flip flop" shoes and heavy work boots in-patient care areas. Appropriate stockings and/or hosiery should be worn.

Name badges must be worn and fully visible at all times. Reference Personnel Policy 5300-08 #3 Parameters.

A staff member reporting to work in violation of this Policy will be instructed by the Director/Manager/Supervisor to return home, without pay, to change, or to make other modifications in attire, grooming, accessories and/or makeup, etc., to comply with these standards.

2. Clothing Guidelines

Associates working in office areas are to wear clothing, which presents a business-like appearance.

Prohibited clothing includes, but is not limited to, the following items for all associates in all departments:

- a. Sunglasses, unless worn for medical reasons.
- b. Hats, scarves, when used as a head covering. Scarves may be used to tie hair back. Hats and turbans of a religious or cultural nature will be acceptable as well as associates undergoing medical treatment.
- c. Tee shirts expressing verbal sentiment or personal expression.,i.e., advertisements, etc. Single-color tee shirts, crew neck or v-neck are permitted under scrub suits.
- d. Hemlines shorter than one (1) inch below fingertip length above the knee.
- e. Revealing clothing or styles (see-through, low cut).
- f. Bare midriffs or backless attire. No Capri's.
- g. Sweatshirts, or sweat pants, including "designer" styles or collared sweatshirts.
- h. Dungarees, overalls, or jeans, including "designer" jeans. An exception: Maintenance department associates are permitted to wear jeans, and or appropriate jumpsuits.
- i. Visible tattoos, facial jewelry, such as eyebrow rings/studs, nose rings/studs, lip rings/studs or tongue studs are not considered appropriate or professional in the medical center work environment. This kind of jewelry is not to be worn during work time. Additionally, excessive (more than 2 sets) of earrings are also discouraged. Earrings should be small in size.
- j. Any attire judged to be suggestive, immodest or inappropriate by supervisory personnel.

3. Specific Uniform Clothing Requirements

a. Uniformed Departments

Specific departments may require employees to wear standard uniforms. These departments include, but are not necessarily limited to: Security, Materials Management, Nutritional Services, Maintenance, Engineering and Patient Care Units.

Other individual departments may specify requirements for wearing surgical scrub suits within their work areas.

b. Departmental Dress Codes

Individual departments are encouraged to have dress code policies specific to their departments that are in accord with this policy. Copies of such departmental policies will be placed next to this policy in departmental manuals. Originals of departmental policies are to be forwarded to Human Resources for inclusion in the master Personnel Policy.

1. Grooming

All staff members' hair must be kept neat and clean. Depending on a staff member's assigned duties or work area, he or she with long hair may be required to tie their hair back, or wear a hair net. Male staff will be clean-shaven, or if a beard or mustache is worn it must be well groomed.

Staff must use good personal hygiene.

2. Accessories and Makeup

Flashy jewelry may present a safety hazard to patients and coworkers. Makeup and nail polish should not be extreme. Regulations of specific departments may require that nail polish not be used. Staff in direct patient care must refrain from long fingernails.

3. Fragrances

Some patients, coworkers and visitors may be sensitive or allergic to certain types of fragrances. Staff must use these substances at a minimum and with discretion.

4. Name Badges

Name badges must be worn at all times so that patients, visitors, and employees can identify staff and their job title.

5. Non-Compliant

Should a staff member report to work improperly dressed or groomed, the Department Director/Manager/Supervisor will instruct them to return home to change. Staff will not be permitted to work when they are improperly attired.

An employee, when sent home, will not be compensated for the time they are away from work.

Continued problems may result in disciplinary action.

POLICY/PROCEDURE

FACILITY: LHN
DEPT. NO: 01.8650
POLICY NO: 5300.06
DEPARTMENT: Human Resources
TITLE: Dress Regulations and Appearance

PRINT NAME (ABOVE)	PRINT POSITION (ABOVE)
SIGN (ABOVE)	DATED AT PASCO, WASHINGTON

POLICY/PROCEDURE

FACILITY: LHN
DEPT NO: 8612/8611
POLICY NO: 21/ C-3
DEPARTMENT: Board of Directors/Administrative
TITLE: Corporate Responsibility Program: Investigation and Reporting Protocols

STANDARD: To establish an effective corporate responsibility program conducive to compliance with applicable laws and regulations, policies and procedures of Lourdes Health Network. The corporate responsibility officer (CRO) is designated by the Chief Executive Officer and senior management. The CRO and the Corporate Responsibility Committee are accountable to senior management.

POLICY: The Board of Directors shall establish a Network Corporate Responsibility Program that focuses, both with respect to individuals and organizations, on business and professional standards of conduct; compliance with federal, state and local laws; promotion of good corporate citizenship; prevention and early detection of misconduct; identification/prioritization of high risk areas; and communication/education for associates and agents. The CRP shall be designed to prevent, detect, and report actions by employees, agents, and professionals that constitute violations of applicable laws, regulations, policies and procedures. The CRO shall ensure annual education on Corporate Responsibility regulations is completed. LHN Corporate Responsibility Program includes provisions for internal and external monitoring and auditing.

PROTOCOLS: These protocols have been developed to assist the Corporate Responsibility Officer (CRO) in appropriately responding to and correcting potential compliance program. The CRO shall maintain effective lines of communication with the organization's associates. When conducting an investigation, judgment should be exercised and consideration should be given to the scope and materiality of the potential violation. A prompt investigation conveys to the government that Lourdes Health Network (LHN) takes the Corporate Responsibility Program seriously.

These protocols also address the use of system counsel. In an effort to promote consistency among its Health Ministry in regards to compliance investigations, Ascension Health has determined that system counsel should be involved in most investigations that are determined to be serious or potentially serious. This decision is not meant to completely exclude the sue of local counsel, but to provide, at a minimum, oversight that will ensure consistency in how investigations are handled, including decisions regarding repayment and self-reporting.

1.0 A reporting party discovers or learns of a potential violation of a law, regulation, or the Ascension Health/Lourdes Health Network/Lourdes Health Network Standards of Conduct. Sources of learning of potential violations may include audits or self-monitoring programs, the government, current associate, former associate or independent contractor.

Original Effective Date:	1998	
Original Dept.	Admin/Board/RM	Supercedes:
Date of Revisions:		Date of Reviews
Admin/Board	2/03; 7/05	11/98; 11/00; 10/02; 8/04; 9/06
QM	2/03; 5/05, 10/05	

- 1.1 The party discovering or learning of a potential violation has an affirmative duty to report the potential violation to one of the following:
- His/her supervisor;

- The LHN CRO or his/her designee; or
- The Ascension Health Hotline Service

1.2 The individual taking the report will inform the reporting party(ies) of the confidential nature of the report, but will also communicate that an individual's identity may have to be revealed in certain instances for example, if governmental authorities become involved.

2.0 Supervisor: The supervisor will notify the LHN CRO within 24 hours of receiving notification of a potential violation. Notification should occur in person or via telephone. The reporting party and their supervisor must not document nor discuss the situation with other associates or outside parties.

Ascension Health Hotline Service: The Ascension Health Hotline Service will document discussions with reporting parties by completing a disclosure reporting form. The disclosure reporting form completed by the Ascension Health Hotline Service will be provided to the LHN CRO within 24 hours of receiving notification of a potential violation.

Hospital CRO or Designee: The LHN CRO will document the circumstances on the Ascension Health disclosure reporting form, referred to as the Confidential Corporate Responsibility Report (CCRR), or an equivalent document. If the report was received through the Ascension Health Hotline Service, a copy of the hotline's disclosure reporting form will be attached to the CCRR. There will be prompt responses to detected offenses, and for development of corrective action initiatives.

3.0 The LHN CRO makes a determination as to whether the situation documented on the CCRR form represents a serious or potentially serious violation. In some cases this will be readily evident, and in others the LHN CRO may need to conduct a cursory investigation to determine the potential impact of the reported issue. Serious violations are those that could result in significant civil liability, criminal prosecution, and/or exclusion from Medicare or Medicaid programs or other major sanctions. While it is difficult to quantify serious or potentially serious, any issue with a potential impact of \$100,000 or more would fall into this classification. Examples may include billing errors (\$100,000 to all payors combined), underreporting of taxes, private inurement, excess benefit, cost reporting issues, etc. Overpayment situations involving federal or state programs are generally deemed serious in nature.

3.1 If the potential violation is determined **not** to be serious, then the LHN CRO will coordinate an investigation with assistance of either local or system counsel, as determined by the LHN CRO.

3.1.1 Questionable practices will cease immediately upon knowledge or clear indication of a violation (e.g., stop billing inappropriately if discovered).

3.1.2 Upon investigation, the LHN CRO may determine that a Corrective Action Plan is necessary. Specific steps in the Corrective Action Plan may include revision of a policy and/or procedure, additional education and training for an identified risk, specific steps to be taken related to the particular problem, and/or other actions

as deemed necessary by the CRO. Other management staff may be involved in corrective actions.

3.1.3 The investigation will be thoroughly documented in a systematic manner.

3.2 If the potential violation is determined to be serious or potentially serious, the LHN CRO must notify the

3.2.2 LHN CEO, in-house counsel and the Ascension Health CRO.

3.2.1 A copy of the CCRR and Ascension Health Hotline Service disclosure reporting form (if applicable) will be provided to the Ascension Health CRO.

3.2.2 Legal counsel will be involved in all serious or potentially serious issues. Options include the use of system counsel alone, the use of local counsel in conjunction with system counsel, and the use of local counsel alone.

3.2.3 The LHN CRO and the Ascension Health CRO will make a determination regarding the need to involve system counsel, including which law firm would be most appropriate for the issue at

hand. Designed system counsel has been defined as Garnder, Carton & Douglas or Hall, Render, Killian, Heath & Lyman.

- 3.2.4 There may be cases where it is appropriate to have local counsel participate in the investigation in conjunction with or in lieu of system counsel. A determination will be made jointly by the LHN CRO and the Ascension Health CRO. If a decision is made to use local counsel in conjunction with system counsel, the responsibilities of local counsel versus system counsel will be clearly documented in writing by the LHN CRO and will be provided to the Ascension Health CRO. We anticipate that system counsel would, at a minimum, act in an oversight role on the majority of serious issues. This would include reviewing corrective action plans and making recommendations regarding repayment and self-disclosure, if warranted.
- 3.2.5 Ascension Health will pay the legal fees associated with the initial contact to system counsel, if any. If, as a result of that contact, it is determined that there is a need for continued involvement by system counsel, all subsequent legal fees associated with that issue will be the responsibility of the LHN. All legal fees incurred by local counsel continue to be the responsibility of the LHN.
- 3.2.6 Regardless of whether system or local counsel is utilized in an investigation, the use of internal resources is highly recommended to minimize legal/consultant fees. Internal resources may include the use of in-house counsel (as appropriate), the use of internal expertise to research the issue and perform preliminary analyses, and the use of the Catholic Healthcare Audit Network

(CHAN) to develop audit methodology, perform the audit, report on findings and draft corrective action plans.

- 3.2.7 In all cases, the ultimate oversight of and responsibility for the investigation rests with the LHN CRO. This includes approval of all corrective action plans and decisions regarding repayment and self-disclosure, if warranted.

- 3.3 If the potential violation is determined to be serious or potentially serious, the Ascension Health CRO will notify the Ascension Health Senior Vice President, Legal Services and General Counsel.

- 4.0 For serious or potentially serious violations, the LHN CRO and designated legal counsel will develop an investigation plan.

- 4.1 An investigation plan should define the scope of the potential problem, including the period that will be investigated (may be less than the time the situation has existed), sampling methodology, additional resources necessary to complete the investigation, and an estimation of the potential financial impact.

- 4.2 The LHN CRO will consider, based on consultation with the Ascension Health CRO, whether CHAN or an outside consultant is needed and appropriate to perform an audit.

- 4.2.1 In the event an independent audit is deemed necessary, a letter of engagement will be sent by the appropriate legal counsel to keep the investigation under the attorney-client privilege to the extent possible. If CHAN performs the audit, the engagement letter should be addressed to the CEO of CHAN rather than the local auditor.

- 4.3 Questionable practices will cease immediately upon knowledge or clear indication of a violation (e.g., stop billing inappropriately if discovered).

- 4.4 The investigation will be thoroughly documented in a systematic manner.

- 5.0 Based on the findings from the investigation and input from the Ascension Health CRO, system counsel and other involved parties, a detailed Corrective Action Plan will be developed. Components of the Corrective Action Plan must include issue identification, the findings, the recommendations, those responsible for follow-up and a target date for completion.

- 5.1 Corrective Action Plans for serious or potentially serious violations will be approved by the LHN CRO and management, with a copy forwarded to the Ascension Health CRO.
- 5.2 The LHN CRO is responsible for monitoring the implementation and effectiveness of the Corrective Action Plan.
- 6.0 At the conclusion of an investigation, the LHN CRO will discuss with the Ascension Health CRO and designated counsel whether a voluntary self-disclosure obligation exists.
- 6.1 If there is an obligation to self-disclose to the government, the LHN CRO and designated counsel will determine how and when to make the disclosure.**
- 6.2 If no disclosure responsibility exists, proceed with the reporting requirements described below.
- 7.0 The LHN CRO is responsible for reporting the results/status of investigations to the local CRP Committee and the local Audit Committee, as well as to the Ascension Health CRO.
- 7.1 The level of information provided to the CRP Committee about specific investigations will be left to the discretion of the LHN CRO. At a minimum, the CRP Committee should receive periodic reports on the number of reported violations, the number confirmed, and the number requiring a corrective action plan. These summary reports should include both serious and non-serious violations.
- 7.1.1 For investigations performed under Attorney-Client Privilege, specific details of the investigation would be limited to a verbal presentation to the CRP Committee regarding the general nature and content of the reports.
- 7.2 The LHN CRO will provide summary reports (typically three to four times per year) to the Audit Committee. These summary reports should include both serious and non-serious violations. See Attachment 6 to Appendix B of the Ascension Health CRP Manual for guidance and examples of reports to governing Boards and Board committees.
- 7.2.1 For investigations performed under Attorney-Client Privilege, specific details of the investigation would be limited to a verbal presentation to the Audit Committee regarding the general nature and content of the reports.
- 7.3 For investigations into serious or potentially serious issues, copies of the completed CCRR (or an equivalent document) and final audit reports, if applicable, will be forwarded to the Ascension Health CRO.
- 7.4 The Ascension Health CRO, or his designee, will prepare periodic reports summarizing investigations that were either initiated by or disclosed to governmental agencies. This summary will be provided to the Senior Vice President of Legal Services, Ascension Health Divisional Executives and the Ascension Health Audit Committee.**
- 8.0 LHN CRO is responsible for informing the original reporting party that corrective action has been taken. However, certain specific steps taken may need to remain confidential because of employment sensitive nature of information based on attorney-client privilege. The extent of information provided to the disclosing party should be the responsibility of LHN CRO using his/her discretion.
- 8.1 Parties that reported potential violations through the use of Ascension Health Hotline Service will receive follow-up reports through the service whenever possible. Parties that reported potential violations through other means will receive feedback directly from the LHN CRO.**
- 9.0 LHN associates who violate the Standards of Conduct shall be subject to disciplinary action up to and including termination.
10. The Corporate Responsibility Committee, which is chaired by the LHN CRO, meets on a monthly basis. The CRO provides updates to the Audit Committee on a quarterly basis.

POLICY/PROCEDURE

FACILITY: LHN
DEPT NO: 8612/8611
POLICY NO: 21/ C-3
DEPARTMENT: Board of Directors/Administrative
TITLE: Corporate Responsibility Program:
Investigation and Reporting Protocols

I understand that my obligations under this Agreement will continue after termination.

PRINT NAME (ABOVE)	PRINT POSITION (ABOVE)
SIGN (ABOVE)	DATED AT PASCO, WASHINGTON

Original to be placed in Personnel File or other appropriate file.

Abuse/Neglect Fact Sheet

I.

Abuse: the willful infliction of injury, unreasonable confinement, intimidation, or punishment with resulting physical harm, pain or mental anguish.

Examples of Abuse:

Verbal Abuse: Any use of oral, written or gestured language that willfully includes threats and/or disparaging and derogatory terms to our patients, families and/or employees. Stating things that may frighten someone.

Sexual Abuse: Inappropriate touching, sexual harassment, sexual coercion, or sexual assault.

Physical Abuse: Hitting, slapping, prodding, poking, pushing, shoving, pinching, etc. a patient. Withholding food and medications.

Mental Abuse: Humiliation, harassment, threats of punishment or deprivation.

Involuntary Seclusion: Isolating a person against the residents will or leaving them in an isolated location.

Willful Deprivation by Inaction: Refusal of staff to intervene or assist a patient when asked.

Neglect:

1. A pattern of conduct or inaction by a person or entity with a duty of care to provide the goods and services that maintain physical health of a vulnerable person, or that avoids or prevents physical or mental harm or pain to a vulnerable person.
2. An act of omission that demonstrates a serious disregard of consequences of such a magnitude as to constitute a clear and present danger to the vulnerable persons health, welfare or safety.

Examples of Neglect may include, but are not limited to the following:

- Failure to carry out orders for treatment, therapy, diagnostic testing, administration of medications,
- Failure to answer a call light in a reasonable time frame when the condition of the patient warrants a timely response
- Being left to sit or lie in urine or feces
- Failure to feed or assist a patient who requires help with feeding

II

Investigation Process:

Critical components:

- Timeliness of the initiation of the investigation-you are expected to report immediately.
- Thorough investigation to include: who, what, when & where. Also the how & why.
- The investigator needs to be the objective.

III

Protection: Immediate removal of the alleged source of abuse/neglect from the workplace until the investigation is completed.

IV

Reporting Requirements:

Who

- Any employee who observes and incident or hears the victim state what happened
- Any employee who hears about an incident from a permissive reporter

Where to report

- To your director or designee
- To appropriate agency. Refer to policy & procedure A-1 in *Administration Manuel*.

What to report

- Any reasonable cause to believe an incident of abuse/neglect has occurred
- Any suspected incident of abuse/neglect

When to report

- As soon as possible

Abuse/Neglect
Annual Training
(REMEMBER TO REVIEW SEPARATE FACT SHEET)

Print Name:

Dept:

Date:

Please circle the appropriate answer:

1. Abuse is only physical.
True False

2. Threats of punishment are what type of abuse?
Verbal Sexual Physical Mental Involuntary

3. Failure to answer a call light is an example of:
Abuse Neglect

4. When is a report of abuse/neglect to be reported?
 - a. Immediately
 - b. After the incident is investigated

5. Who is to report an alleged incident of abuse/neglect?
 - a. Your director
 - b. The PCC
 - c. You
 - d. None of the above

6. Any suspected incident of abuse/neglect is to be reported.
True False



Lourdes Health Network

POLICY/PROCEDURE

FACILITY: LHN
 DEPT NO: 01.8650
 POLICY NO: 5300.03
DEPARTMENT: Human Resources
TITLE: Confidentiality

STANDARD: To identify the procedure for imposing disciplinary or corrective action as a result of an associate's failure to comply with LHN's Confidentiality/Privacy/Security Program Policy and Procedures.

To identify certain Uses and Disclosures of Protected Health Information (PHI) that would not result in disciplinary or corrective action.

POLICY: This Confidentiality/Privacy/Security Program policy of Lourdes Health Network (LHN) applies without limitation to any associate, or organization acting as an agent of LHN, whether paid or unpaid, otherwise associated with or providing services for LHN, including hospital associates, corporate associates, contracted associates, volunteers, students, and physicians and other health care providers. LHN will impose appropriate disciplinary or corrective action against any individual or organization that violates LHN's Confidentiality/Privacy/Security policies. Protecting the confidentiality of patient demographic and medical information; corporate and proprietary information; and printed, written, oral or electronic records, is an obligation of all LHN's workforce. Protected information must be released to any individual, organization or agency that the associate reasonably believes has proper authorization or in accordance with federal and state laws. However, inappropriate or unauthorized release of confidential information, or any violation of this policy, may result in immediate corrective or disciplinary action, including termination of employment, service, or association with LHN.

PROCEDURE:

Use or Disclosure of PHI by an associate in violation of LHN's Confidentiality/Privacy/Security Program Policy and Procedures will result in disciplinary or correction of the associate as appropriate to the nature of the violation. The action may range from warning to termination and will be determined by LHN based on all the relevant facts and circumstances.

Original Effective Date:	06/01/75	
Original Dept.	Human Resources Administration: 11/97;11/01;04/04 Medical Records: 11/97 Risk Management: 11/97;04/04;7/06 Information Systems: 11/97;7/06 Amburgey & Rubin: 04/04 Privacy & Information Technology: 12/05;7/06	Supersedes: LMC Pol #: 5300.02; 11/97 LCC Pol #: 414.5; 11/97
Dates Revised:	12/85;5/87;11/97;11/01;4/04;12/05;7/06	Dates Reviewed: 11/84; 8/86; 8/87; 9/89; 1/93; 3/96; 11/97; 11/99; 5/04; 6/07; 5/08;4/09

CONFIDENTIALITY/PRIVACY/SECURITY OF INFORMATION

1. This policy will apply to:

Any associate or organization acting as an agent of LHN whether paid or unpaid, otherwise associated with or providing services for LHN whether hospital associates, corporate associates, contracted associates, volunteers, students, or physicians.

Any associate who obtains access to confidential information as the result of job duties, training, education, and auditing, investigative or volunteer activities, regardless of the location where such activities take place.

This policy is not intended to interfere with the right of associates to communicate with their exclusive bargaining representative (e.g., union representative or shop steward) about appropriate issues.

Any outside agency or organization that LHN has granted authorized electronic access, e.g., Lourdes medical, personnel, financial, or other record keeping or data storage systems will be required to sign a Confidentiality Agreement. Refer to page 6.

Patient Information

Whether personal, medical, financial or statistical and including:

- a. Written, oral, printed, or electronic patient records;
- b. Conversations about patients that may be overheard by others, e.g., telephone, on breaks, in elevators, cafeteria, nurses' stations, etc.

Associate Information

All information contained in personnel files and on electronic systems including, but not limited to, salary information, disciplinary actions, EEO charges, garnishments, investigatory actions, personal information, e.g., home phone, address, age, date of birth, SSN, other protected class information, or associate health information.

Proprietary Trade Information (includes):

LHN strategic plans, written or unwritten.

LHN Financial and statistical records.

LHN Marketing strategies and activities, written or unwritten.

LHN Internal memos and communications not intended for public use.

2. Uses and Disclosures

All information regarding patients' medical care, associate records, and proprietary trade is confidential and is to be maintained as such.

No health care worker will have access to, or the right to review patient or associate records, or disclose personal or medical information, except when necessary to provide medical care or for administrative purposes. Each associate will have access to the minimum necessary to perform work as determined by the Department Director/Manager/Supervisor.

Sharing or misusing electronic passwords is prohibited. Any occurrence, including incidental or accidental breaches of confidentiality, involving electronic passwords or security shall be reported immediately to the Corporate Compliance Officer, Privacy Officer, Security Officer and Human

Resource Director. The Corporate Compliance Officer and Privacy Officer will follow up with appropriate Department Directors/Managers/Supervisors if necessary.

Personal information, e.g., address, phone number, and associate health records, will not be released except by the associate or with the associate's consent, except for disclosures that are required by law or that LHN considers necessary or appropriate for the proper conduct of its business.

In the event a patient is an outpatient or admitted to LHN services, PHI received at time a patient is admitted as an outpatient or inpatient, during the course of patient's hospital stay, or at discharge, may not be released without an appropriate signed consent or as required by law unless the disclosure is required by law or LHN decides the disclosure is necessary or appropriate for the proper conduct of its business.

Applicable consent laws regarding Disclosure of Information will be followed, e.g., HIV infection, billing, etc.

Discussion, transmission, or disclosure of patient or associate information will occur only as necessary to provide medical care, as LHN staff considers necessary or appropriate to carry out its health care and business operations. PHI may be shared among LHN for the

purpose of providing continuity of care to the patient unless the law prohibits such sharing. Such PHI will be maintained in a confidential manner in accordance with this policy.

Verbal communications or discussion by LHN staff/associates with any person will be conducted in a manner to ensure privacy or protect confidentiality unless circumstances do not permit such communication.

During orientation, each associate will be instructed in the correct procedures and requirements regarding confidential information.

Any violation of this policy will constitute grounds for immediate sanctions and may include termination of employment, service, or association with LHN.

3. Unauthorized Use or Disclosure of Personal Health Information (PHI).

All Uses and Disclosures of PHI by an associate in violation of LHN's Confidentiality/Privacy/Security Program Policy and Procedures shall be reported to the Privacy Officer, Corporate Compliance Officer and/or Security Officer who, in accordance with LHN's Personnel Policies and Corporate Responsibility Program, will determine the appropriate action to be taken.

If it is determined that a violation has occurred, the Privacy Officer and Security Officer in conjunction with the Corporate Compliance Officer, employee's manager and Human Resources Director will:

- a. Carry out or recommend appropriate disciplinary or corrective action;
- b. Identify any changes or additions to policy and procedures and education that may help prevent future occurrences or violations of a similar nature;
- c. Oversee the implementation of the recommended changes or actions to the extent practical;
- d. Identify any harm that may have been caused to the associate as a result of the violation;
- e. Oversee the mitigation of the harm to the extent practical.

In determining the appropriate action, the circumstances of the violation will be considered, including, without limitation:

- a. The nature and severity of the violation;
- b. Whether the violation was intentional or unintentional;
- c. Whether the violation represented an isolated occurrence or a pattern of unauthorized Use and Disclosure of PHI;
- d. Any history of past violations or disciplinary actions;
- e. The action taken in response to similar violations;
- f. The workforce member's willingness to cooperate with investigation of the violation.

The Privacy Officer will document the action taken and will retain such documentation for six (6) years from the time the document was created.

4. Disclosures of PHI that will not Result in Sanctions

a. Disclosure by Whistleblowers

Any Disclosure of PHI by an associate, acting as a whistleblower, to a health oversight agency, appropriate public health authority, or the associate's attorney, will not subject the associate to sanctions for violation of LHN's Confidentiality/Privacy/Security Policy and Procedures, provided the associate, in good faith, reasonably believes that LHN has acted unlawfully, violated professional or clinical standards, or potentially endangered a patient in providing care or service.

b. Disclosure by Victims of Crimes

An associate will not be subject to disciplinary or corrective action for violation of LHN's Confidentiality/Privacy/Security Program Policy and Procedures if the associate is a victim of a crime and discloses to law enforcement official or to the associate's attorney, the following PHI about the suspected offender:

- i. Name and address
- ii. Social Security Number
- iii. ABO blood type and Rh factor
- iv. Type of injury
- v. Date and time of treatment
- vi. Date and time of death, if applicable, and
- vii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

c. Other Disclosures

An associate will not be subject to disciplinary or corrective action for violation of LHN's Confidentiality/Privacy/Security Program Policy and Procedures if the associate:

- i. Files a complaint with the Secretary of DHHS pursuant to the HIPAA Regulations;
- ii. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act; or
- iii. Opposes any act or practice as unlawful under the HIPAA Regulations, if the workforce member has a reasonable, good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Regulations.
- iv. Discloses information in reasonable reliance on the direction from a Director/Manager/Supervisor of LHN.

5. Examples of Breaches of Confidentiality

a. Accessing information that is not within the scope of the associate's job:

- i. Unauthorized reading, copying, downloading, etc., of patient account information.
- ii. Unauthorized reading, copying, downloading, etc., of patient electronic or physical record.
- iii. Unauthorized access to personnel file information.
- iv. Accessing information that you do not need to know for the proper execution of your job.

b. Disclosing to or using:

- i. Another associate's protected information, sign-on code, or password for accessing electronic records.
- ii. Disclosing to a co-worker your password or using a co-worker's password.
- iii. Disclosing to an unauthorized person the access codes for personnel files or patient accounts.
- iv. Making unauthorized use of a login code for access to personnel files or patient accounts.
- v. Disclosing to any unauthorized person and/or person's matters of proprietary trade information.

- vi. Discussing or disclosing confidential information in a public area, such as a waiting room, cafeteria, elevator or with persons who do not have a need to know in order to carry out their duties.

c. Leaving a secured computer application unattended while signed on:

- i. Not "logging out" when away from workstation.
- ii. Allowing a co-worker to use your log on to access secured application to which he or she does not have access.
- iii. Attempting to access a secured application without proper authorization.
- iv. Trying passwords and log on codes to gain access to an unauthorized area of the electronic system.
- v. Using a coworker's application for which you do not have access after he or she is logged in.

d. Unauthorized use or alterations of patient or personnel information:

- i. Making unauthorized marks on a patient's chart or in the electronic medical record.
- ii. Making unauthorized changes to or deletions from a personnel file.
- iii. Producing or sharing information in a patient chart or a personnel file with unauthorized persons.

6. Sanctions for Breach of Confidentiality

a. If an associate looks at his/her own patient record(s) without first signing an authorization through the medical record department the following steps ordinarily shall be taken:

- Step 1 - Verbal warning with retraining
- Step 2 - Written warning
- Step 3 - Suspension
- Step 4 - Termination

b. If an associate breaches confidentiality, the following steps will ordinarily be followed:

- Step 1 - Written warning
- Step 2 - Termination

PRIVACY AND INFORMATION TECHNOLOGY USER AGREEMENT
BY AND BETWEEN LOURDES HEALTH NETWORK'S
ASSOCIATES, CONTRACTORS, MEDICAL STAFF, VOLUNTEERS, AND STUDENTS

Privacy of patient information, personal, medical, financial statistical; corporate and proprietary information; and human resource information is the obligation of all Lourdes Health Network (LHN) associates, corporate associates, contracted associates, volunteers, students, physicians and other healthcare providers. Private information, which is any information learned on the job, in oral, written, printed, or electronic form, must not be or disclosed to any individual, organization or agency without valid written authorization, except as allowed by federal or state law.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires protection of confidential information contained within our information systems. Inappropriate disclosure of client data may result in the imposition of fines up to \$250,000 and ten-year imprisonment per incident.

Accordingly, as a condition of, and in consideration of my access to confidential information and systems

I will:

1. Follow all LHN's Confidentiality/Privacy and Security Programs Policy and Procedures. I understand that sanctions listed in Personnel Policy 5300-03 will be applied for violations. I understand that civil and criminal penalties may also result for privacy violations.
2. Accept responsibility for all activities undertaken using my User-ID, password, PIN or other access code or authorization.
3. Protect my User-ID and password as LHN restricted information. My User-ID is assigned to me alone and will not be shared with anyone, including co-workers, trainers or other personnel.
4. Be held responsible for my misuse or wrongful disclosure of confidential information and for my failure to safeguard my User-ID, password, PIN or other access code or authorization for access.
5. Log off, lock or invoke a password-protected screensaver when away from my workstation.
6. Not auto-forward any LHN email to any non-LHN account unless I have received authorization from the Director of Information Systems.
7. Not visit "High Risk" Internet sites or sites containing content that could cause damage or bring embarrassment to LHN.
8. Acknowledge that I understand information, which is composed, transmitted or received via LHN IT assets, is considered to be part of the official records of LHN and, as such, is subject to disclosure law enforcement, government regulators or other third parties (i.e., may be subpoenaed.)
9. Be responsible for the correct and proper use of the tools each system provides for maintaining the security and confidentiality of information stored on it.
10. Be aware of the potential harm caused by computer viruses and other destructive computer programs and will take steps to avoid being their victim or unwitting vector.

11. Immediately report any accidental or unintentional access to discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive information to my supervisor, the Privacy Officer, the Security Officer and/or Corporate Compliance Officer.
12. Notify Human Resources and/or Department Director/Manager/Supervisor of any situation change, such as employment termination or change in job status that would make my continued access to and use of LHN private information inappropriate.
13. Access company information only in the conduct of LHN business.
14. Secure sensitive company information in my work area at the end of the day in order to protect it against unauthorized access and/or theft. (e.g., at the end of the day or when on a trip.)
15. Respect the confidentiality and privacy of individuals whose records may be accessed.
16. Observe any ethical restrictions that apply to information to which I have access, and to abide by applicable laws or policies with respect to access, use or disclosure of information.

17. Not disclose information labeled as LHN Internal, Confidential or Restricted or distribute such information in any medium, unless the recipient's authorization has been verified and the means of transmission is appropriate.
18. Not access or use any company information for my own personal gain or profit, or the personal gain or profit of others, or to satisfy personal curiosity.
19. Not access LHN resources for illegal purposes including but not limited to intentional harassment of other users, intentional destruction of or damage to equipment, intentional disruption or unauthorized copying of copyrighted materials.
20. Respect all copyrights and licenses associated with LHN Information Technology (IT) systems. I will not remove any company-owned or licensed software from the facility without appropriate authorization from the Director of Information Systems.

I understand that my access to LHN systems is a privilege and not a right afforded to me.

I understand that if I fail to abide by LHN policies, standards or procedures, my access privileges may be suspended or revoked, administrative action may be taken, I may be dismissed (where appropriate) and I could be prosecuted in civil or criminal court.

I understand LHN may audit all events relative to my User-ID, monitor my network/Internet usage, and may retrieve/read any information composed, sent or received through online connections and stored in LHN IT systems. (e.g., files, email.) (Note: Privacy of information processed, stored or emailed on LHN computers and information systems is neither implied nor expected.)

I understand and agree to abide by the conditions outlined in this agreement. (Note: Failure to accept these standards of behavior means that I will not have access to any LHN IT assets, which may be grounds for my dismissal.)



Lourdes Health Network

POLICY/PROCEDURE

FACILITY: LHN
DEPT NO: 01.8650
POLICY NO: 5300.03
DEPARTMENT: Human Resources
TITLE: Confidentiality

I understand that my obligations under this Agreement will continue after termination.

PRINT NAME (ABOVE)	PRINT POSITION (ABOVE)
SIGN (ABOVE)	DATED AT PASCO, WASHINGTON

Original to be placed in Personnel File or other appropriate file.

**TERMINATION NON-DISCLOSURE AGREEMENT FOR
ASSOCIATES, CONTRACTORS, MEDICAL STAFF, VOLUNTEERS, AND STUDENTS**

Lourdes Health Network has a legal and ethical responsibility to safeguard the privacy of all patients and protect the confidentiality of their health information. In the course of my employment/assignment at Lourdes Health Network, I may have come into possession of or overheard confidential patient information, even though I may not have been directly involved in providing patient services.

I understand that such information must be maintained in the strictest confidence. I hereby agree that I will not at any time during or after my employment/assignment with Lourdes Health Network disclose any patient information, in any form, to any person whatsoever.

I understand that violation of this agreement may result in civil and criminal penalties.

PRINT NAME ABOVE	PRINT POSITION ABOVE
SIGN ABOVE	DATED AT PASCO, WASHINGTON
WITNESS PRINT NAME ABOVE	WITNESS SIGN ABOVE

Original to be placed in Personnel File or other appropriate file