

DEPARTMENT OF VETERANS AFFAIRS
NEW YORK HARBOR HEALTHCARE SYSTEM

MANDATORY TRAINING MANUAL

INTRODUCTION

This manual will acquaint you with essential information to ensure that your experience at New York Harbor Healthcare System (NYHHS) is both safe and rewarding. The topics covered are annual mandatory training requirements for trainees, contract and consultant or fee basis staff as well as part-time and full-time staff. Mandatory training may also be completed by accessing NYHHS's Online Employee Education System intranet website.

To ensure you are credited with completion of this training, you must return a completed competency test and signed certificate to your VA Service Office or the Medical Staff Office before your initial rotation or session of service, before reappointment to the medical staff or by the due date specified upon transmittal of this manual. The test and certificate are on pages 61-64. You may return these pages by fax, mail or delivery to the VA Service Office or the Medical Staff Office.

On its intranet website, NYHHS maintains a compendium of healthcare system policies that detail approved operating procedures for particular situations important for patient care. Policies can be found by accessing the healthcare system's home page on the intranet and selecting FORMS AND PUBLICATIONS and then POLICIES under the heading NYHHS ADMINISTRATIVE FORMS AND DOCUMENTS. House staff and others involved in inpatient care should familiarize themselves particularly with the policies on Blood Transfusions (No. 113-2) and Restraints and Locked Seclusion (No. 11-37).

CONTENTS

MISSION, VISION & VALUES	3
INFECTION CONTROL	4
FIRE PREVENTION.....	7
HAZARDOUS MATERIALS	8
GENERAL SAFETY	10
UTILITIES SYSTEMS	12
EMERGENCY MANAGEMENT	13
SECURITY MANAGEMENT	14
WORKPLACE VIOLENCE AWARENESS & PREVENTION	15
OCCUPATIONAL HEALTH.....	16
GEMS.....	18
INFORMATION SECURITY AWARENESS.....	20
CUSTOMER SERVICE: SERVICE RECOVERY – A STANDARD OF EXCELLENCE	27
DIVERSITY IN THE WORKPLACE	28
SEXUAL HARASSMENT & THE DISCRIMINATION COMPLAINT PROCESS	29
NO FEAR ACT	34
ADR MEDIATION PROGRAM.....	36
LIMITED ENGLISH PROFICIENCY (LEP)	38
PATIENT SAFETY PROGRAM & PERFORMANCE IMPROVEMENT.....	40
RESIDENT SUPERVISION: SUPERVISING PRACTITIONER RESPONSIBILITIES	43
PAIN MANAGEMENT	45
VHA COMPLIANCE & BUSINESS INTEGRITY PROGRAM	46
VHA PRIVACY POLICY TRAINING	48
HEALTHCARE ETHICS.....	53
GIFTS TO HEALTHCARE PROVIDERS FROM THE PHARMACEUTICAL INDUSTRY	54
HEALTHCARE PROVIDERS' EXPECTATIONS OF INDUSTRY & SALES PERSONNEL	57
MANDATORY TRAINING 2009 TEST.....	61
CERTIFICATE OF TRAINING	64

MISSION, VISION & VALUES

OUR MISSION

The Veterans Affairs New York Harbor Healthcare System is dedicated to providing quality health care to veterans using the abilities of all employees supported by our commitment to education and research.

OUR VISION

America's Veterans - the men and women who have defended our freedom are one of our country's greatest sources of pride. These patriots have earned the health care provided by a grateful nation.

We seek to be the provider of choice of veterans and the community by offering an efficient, integrated quality healthcare system capable of providing a full range of primary, specialty and chronic healthcare services in a system that is readily accessible and responsive to change.

OUR VALUES

Trust * Respect * Compassion * Commitment * Excellence * Teamwork * Communication * Diversity

PATIENTS

Our first responsibility is to the patients we serve. We are committed to provide the highest quality care possible.

EDUCATION

We are responsible to provide a learning atmosphere and experience to our patients, staff and students.

RESEARCH

We will encourage the exploration of research and the translation of results to the betterment of patient care.

EMPLOYEES

Our employees are our most valuable assets. They make us what we are. We have a responsibility to treat each employee with respect and dignity.

PERFORMANCE

We will improve our performance by continuing to search for ways to operate more compassionately, efficiently and effectively. We are dedicated to providing timely and courteous service at all times under all conditions in a pleasant and caring atmosphere.

INFECTION CONTROL

HAND HYGIENE

Healthcare workers' hands have been identified as one of the major causes of healthcare-associated infections. The CDC, in conjunction with other organizations, developed guidelines designed to improve hand hygiene practices of healthcare workers and to reduce the transmission of pathogenic organisms. Compliance with CDC Hand Hygiene Guidelines is part of JCAHO's 7th National Patient Safety Goal (NPSG), which requires healthcare organizations to:

- Reduce the risk of health care-acquired infections.
- Comply with current CDC hand hygiene guidelines.
- Manage all identified cases of unanticipated death or major permanent loss of function associated with a health care-acquired infection as sentinel events.

Hand hygiene is the single most important measure to reduce the risk of health care-associated infections. This involves the use of an alcohol-based hand rub or antimicrobial soap and water to routinely decontaminate your hands. Healthcare workers who regularly or occasionally provide direct hands-on care to patients **must not** wear artificial fingernails or extenders.

Procedure for using alcohol-based hand rub:

- Apply product to palm of one hand.
- Rub hands together.
- Cover all surfaces of hands and fingers.
- Rub until hands are dry.
- Do not rinse.

Procedure for hand washing:

- Wet hands with warm water and then add antimicrobial soap.
- Use friction, work up a lather and wash hands for at least 15 seconds.
- Rinse well under a stream of warm water.
- Dry hands thoroughly.
- Turn off faucet using paper towels.

Hands must be washed with antimicrobial soap and water (not with alcohol hand rub):

- When they are visibly soiled or contaminated with blood or body fluids
- After using the restroom
- Before eating
- When caring for patients with *Clostridium difficile* diarrhea

Decontaminate hands with alcohol hand rub (preferred) or antimicrobial soap and water:

- Before and after patient contact
- After contact with blood or body fluids
- Before and after using gloves
- Before inserting and/or manipulating invasive devices (IVs, Foley catheters)
- Between tasks and procedures on the same patient to prevent cross-contamination of different body sites
- After contact with contaminated linen or equipment

STANDARD PRECAUTIONS

Using Standard Precautions means treating all blood and body fluids as if they were potentially infectious. Standard Precautions are designed to reduce the risk of transmission of germs from both known and unknown sources.

Standard Precautions apply to:

- All body fluids except sweat
- Non-intact skin (e.g., cuts, abrasions or draining wounds)
- Mucous membranes

TRANSMISSION-BASED PRECAUTIONS

Transmission-based Precautions are designed for patients known to have or suspected of having a contagious or resistant pathogen. A sign will be placed at the entrance to the patient's room to alert those who enter of the need for special precautions, e.g.:

- Respiratory Precautions (Pink Sign)
- Contact Precautions (Red Sign)

Patients on Transmission-based Precautions should remain in their room. If it is necessary for the patient to leave their room, receiving areas should be notified in advance of the patient's arrival so that appropriate measures may be taken.

Respiratory Precautions (Pink Sign)

- Used in addition to Standard Precautions for patients known or suspected of having TB, measles, chicken pox or disseminated zoster, SARS, or influenza.
- Some of these microorganisms are carried by air currents; others are spread by droplets that can be generated during coughing, sneezing and talking or during procedures.
- N-95 respirator
- Negative pressure room
- Hand hygiene

Contact Precautions (Red Sign)

- Used in addition to Standard Precautions for a patient known or suspected to be infected or colonized with highly infectious or resistant organisms. These organisms can be transmitted by direct contact (skin to skin) or indirect contact (touching) of items or surfaces in the patient's environment.
- Gloves are required and must be put on before entering the patient's room.
- Gowns are to be worn when contact with the patient, his environment or blood or body fluids is anticipated. Gloves and gowns should be removed prior to leaving the patient's room.
- Strict adherence to hand hygiene is required.

PERSONAL PROTECTIVE EQUIPMENT (PPE)

Personal Protective Equipment (PPE) protects you from contact with potentially infectious material. Under normal work conditions, protective equipment should not allow infectious material to contact your work clothes, undergarments, skin or mucous membranes. The type of protective equipment you would select depends on the type of exposure you anticipate. PPE includes:

- Gloves
- Gowns, aprons or lab coats
- Masks or respirators
- Face shields and protective eyewear
- Resuscitation bags or other ventilation devices

FIVE MAJOR TACTICS TO REDUCE THE RISK OF EXPOSURE TO BLOOD BORNE PATHOGENS

1. Engineering controls

Engineering Controls are physical or mechanical systems used to eliminate hazards at the source. Self-sheathing (safety) needles are an example of an engineering control.

2. Employee work practices

Work Practice Controls are procedures you should follow to reduce exposure to blood borne pathogens. Proper use of safety needles is an example of a work practice control.

3. Personal protective equipment

Personal Protective Equipment (PPE) is equipment or clothing that protects you from contact with infectious materials. Gloves, respirators and gowns are examples of PPE.

4. Housekeeping

Careful attention to cleaning your environment protects every healthcare worker. A contaminated sharp carelessly discarded in bedding can cause an injury to EMS or laundry personnel.

5. Hepatitis B Vaccine

Hepatitis B vaccine (HBV) is offered free to all employees. The complete series of HBV is 85% effective at protecting you from getting the disease. You **MUST** decline in writing if you choose to refuse the vaccine.

MANAGING SHARPS INJURIES OR MUCOUS MEMBRANE EXPOSURES

- Clean or flush exposed area.
- Report the incident immediately to your supervisor.
- Report IMMEDIATELY to Employee Health or the Emergency Department. Do not delay.

- If the source of injury is known (e.g., patient or sharp) supply this information to the medical provider. Do not bring the sharp to Employee Health. Use the ASISTS menu to fill out the Incident Report (ask for help if you cannot do it yourself).

TUBERCULOSIS (TB)

Patients known or suspected of having TB are to be placed in a negative pressure room (one in which air flows from the corridor into the isolation room). The windows and doors to the room are to be kept closed to maintain negative pressure. All staff and visitors entering a negative pressure room must wear an N95 respirator. Healthcare workers entering a respiratory isolation room should check the status of the negative pressure by looking at the display monitor found outside of the room. Notify Engineering Service and/or Infection Control for any problems.

Respiratory Protection

If you have not been medically cleared and fit-tested for a respirator, you CANNOT go into a negative pressure room.

What Is the Tuberculin Skin Test (Purified Protein Derivative or PPD)?

- A test to see if your body is carrying the germ that causes TB.
- A small amount of PPD is injected under the skin of your arm.
- A healthcare professional will check the site in two or three days for swelling
- If your test is positive, it does not mean that you have TB or that you are contagious. A positive test means you have been exposed to TB. You may be asked to get a chest x-ray.
- Healthcare workers and volunteers are required to have a yearly TB skin test if they have tested negative in the past.

TB Infection and TB Disease Are Different

- A person with TB infection has the tubercle bacillus, but is not sick and will not spread TB to others.
- A person with TB disease is sick (e.g., has signs of the illness such as coughing, with or without blood tinged sputum, weight loss, night sweats, fever and/or fatigue) and can spread the disease to others.

FIRE PREVENTION

To report a fire or smoke condition:

- At the NY, BK and SA campuses: Call ext. 7000.
- At the CBOCs: Call 911 first, then call ext. 7000.
- Additional emergency telephone numbers can be found on stickers on all the telephones.

All campuses and CBOCs are protected by an automatic fire alarm protection system, including smoke detectors, pull stations and sprinkler systems. When the system is activated:

- At the NY campus you will see strobe lights and hear an alarm tone with an operator announcement.
- At the BK and SA campuses you will hear an alarm tone and automated voice message.

Be aware of fire zones that are separated by smoke barrier doors in your area.

In patient care areas the PCTC/nurse manager or charge nurse is the person in charge. In non-patient care areas follow the directions of your supervisor.

STEPS TO TAKE IN A FIRE: RACE

Rescue Rescue any patients, visitors or staff in immediate danger.

Alarm Pull the fire alarm box. Dial ext. 7000. Notify your co-workers using "Code 7000."

Contain Close all possible doors and windows to delay the fire from spreading.

Extinguish Only attempt to extinguish a fire if you have the proper type of extinguisher and are familiar with its operation. Remember to pull the alarm first before attempting to put out the fire.

Classes of Fire

A – Ordinary combustibles such as wood, paper, plastics and clothing.

B – Flammable liquids/grease, such as greases, oils, gasoline, turpentine and paints.

C – Electrical equipment; any electrical appliance that is plugged in should be treated as energized.

There are various kinds of extinguishers for each class of fire. ABC extinguishers, good for most fires, are the most common types at NYHHS. Extinguishers are only for small fires. They are inspected monthly by Engineering or a service vendor. Know the location of extinguishers in your work area.

Extinguisher Use – The PASS Method

Pull the pin

Aim at the bottom of the fire

Squeeze the trigger

Sweep from side to side

Evacuation

If you must leave the area, move to the next horizontal smoke compartment. You should know where the exits are and where the smoke compartment doors are in your area. If further evacuation is ordered, move vertically to another floor below the area of the fire. Remember, the elevators are not to be used unless directed by the Fire Department. If there are no smoke barriers in your area, **leave the building.**

FIRE DRILLS

The symbol for a fire drill is a sheet of paper stating "fire drill." Employees, residents and students finding the drill symbol should perform all functions exactly as if a real fire exists. (Yes, you are to actually pull the fire alarm to activate the system; during a drill, the signal does not go to the Fire Department so that there is no false alarm.)

HAZARDOUS MATERIALS

Hazardous materials create health and physical hazards.

Health hazards can cause damage to your health if you are exposed to them. Exposure can occur by:

- Inhalation (breathing in)
- Ingestion (eating)
- Skin contact (including eye contact)
- Skin absorption

Types of health hazards include:

- Carcinogens
- Toxic chemicals
- Irritants
- Corrosives
- Sensitizers
- Reproductive toxins
- Target organ toxins that can damage specific parts of your body, such as your liver, kidneys or blood

Physical hazards can cause dangerous situations to occur in the general environment. Types of physical hazards include:

- Combustibles
- Compressed gases
- Explosives
- Any highly reactive materials, especially if they react with air or water

Sources of information on hazardous materials include labeling and Material Safety Data Sheets.

Labeling

All hazardous materials must be labeled. The manufacturer is required to see that all hazardous materials containers are labeled with required information before shipping. You must label the container if:

- The manufacturer's label is damaged or falls off.
- You transfer some of the material to a different container. You must label the new container.

The information on the new label must include:

- Identity of the hazardous chemical(s)
- Health hazards of the product
- Physical hazards of the product

Material Safety Data Sheets

Material Safety Data Sheets (MSDS) are safety fact sheets on hazardous materials provided by the manufacturer. The MSDS for the chemicals that you use in your work area must be available to you during all work hours. They must contain information on:

- Identification
- Hazardous ingredients
- Physical data
- Fire and explosive data
- Health hazards
- Reactivity data
- Spill procedure measures
- Special procedures

The MSDS for the chemicals that you use can be found in the Hazardous Materials Manual (the YELLOW book) in your work area. The written hazard communications program for NYHHS is found in Policy 138-1. A copy of the policy is available on the intranet or through the Safety Office.

Hazardous Chemical Spills

Make sure you always remember to secure/isolate the area around a spill (put up warning signs, put cones or other objects around the spill to prevent staff from walking through it, close and lock doors) and inform other staff of the

spill. This will help prevent people from being accidentally exposed to a hazardous chemical spill because they did not know it was there. Be prepared to provide information on the spill:

- Location of the spill
- Name of the chemical spilled
- Amount spilled
- Any known hazards of the chemical
- If possible and without endangering yourself, have a copy of the MSDS available for the responders.

Small Spills/Leaks

Personnel who are familiar with the hazards involved should use available spill control kits, materials and PPE. When selecting Personal Protective Equipment (PPE) for handling hazardous chemicals, always check the MSDS section on Control Measures. This will tell you what type of gloves, eye/face protection, respirator and other safety equipment is needed to work with the chemical safely. Contact the IH (Industrial Hygienist) for additional information if needed. The following procedures should be followed:

- Contain/isolate the area around the spill.
- Inform your supervisor and other employees in the area of the spill.
- Be sure to wear the correct personal protective equipment.
- Contact the IH to properly dispose of the contaminated materials.

Large Spills/Leaks

The following procedures should be followed when a large quantity of a low or moderately hazardous chemical is spilled or leaked or if a spill or leak of a very hazardous material occurs.

- Contain/isolate the spill; evacuate the area if needed.
- Inform your supervisor and other employees in the area.
- The source of the spill or leak should be stopped immediately, if possible.
- Call Engineering Service:
 - NY campus: daytime shift, ext. 5000; WHEN hours - page #53-183
 - BK campus: daytime shift - ext. 3000; WHEN hours - ext. 3597; also call the telephone operator to request that the EMS shift supervisor be paged
 - SA campus: daytime shift - ext. 2355; WHEN hours - ext. 2222

Emergency Response by NYC Fire Department

For incidents involving hazardous materials, the local NYC Fire Department response units will contact a Hazardous Materials Unit or Radiac personnel.

Hazardous Chemical Spills/Releases at CBOCs

- Contain/isolate the area of the spill. Evacuate if necessary.
- Inform your supervisor and other employees in the area.
- Call the emergency numbers listed for the appropriate campus.
- Be prepared to provide information on the spill to the local Fire Department and VA reps. Refer other inquiries to Public Affairs.

Disposal of Hazardous Chemical Waste

All hazardous chemical waste must be properly disposed of through a permitted waste disposal contractor. Disposal of hazardous chemicals in the garbage, down the sink or through evaporation is against the law.

- Place waste in an appropriate container.
- Do not overfill.
- Label the container with the following information:
 - Hazardous waste
 - Name of the chemical waste
 - Date you started to collect the waste
- When the container is ready for pick up:
 - Contact the IH at the appropriate campus to schedule pick up for proper disposal.
 - Provide the chemical name(s) and the size and number of containers for disposal.

For additional information on the hazardous materials and waste management program, contact the Industrial Hygienists (IH): Ernest Coon, ext. 4130, at the NY campus; Lorraine Laverty, ext. 3587, at the BK campus.

GENERAL SAFETY

SAFETY POLICIES

NYHHS maintains written safety policies, as follows:

Safety Policy Manual (GREEN BOOK)

- Hospital-wide and service-specific safety policies are located in the GREEN Safety Policy Manual.

Hazardous Materials Manual (YELLOW BOOK)

- A list of hazardous materials for each service is maintained in the YELLOW Hazardous Materials Manual. Material Safety Data Sheets (MSDS) provide information regarding hazards of chemicals such as physical properties, health effects, first aid/emergency procedures, etc.

Emergency Management Manual (RED BOOK)

- Emergency management plans are located in the RED book. Employees should be familiar with their role in their service-specific plan during emergency drills as well as actual emergencies.

Safety is every employee's responsibility. Every employee is responsible for knowing the location of the manual in their area.

REPORTING A SAFETY PROBLEM

First, inform your supervisor. If additional assistance is needed, contact: Ernest C. Coon, NYHHS Safety Manager, ext. 3452 at NY campus or at pager 917-762-1007.

Do not take for granted that someone else has already reported the condition. Take the time to call the safety office immediately. Safety is a team effort!

The Environment of Care Committee (EOC) addresses safety issues. It meets every month and is chaired by the Associate Director.

PROPER LIFTING AND BODY MECHANICS

The most common cause of injury among healthcare workers is lifting improperly.

Key points to prevent back injuries:

- Good posture
- Rest
- Good body mechanics
- Proper lifting
- Proper exercise
- Asking for assistance as appropriate
- Use of lifting equipment (e.g., patient lifts)

For good body mechanics:

- Maintain the three natural curves of the back (cervical, thoracic and lumbar) by keeping shoulders, hips, ears, knees and ankles lined up.
- Maintain a wide base of support with feet shoulder-width apart.
- Lift loads close to the body to reduce strain on the back.
- Lift with your legs.
- Keep the muscles of the thighs, abdomen, buttock and back strong to prevent injury.

Make plans before moving/lifting:

- Look over the object to be lifted.
- Inspect the path of travel.
- Plan for distance, space and load.
- Check to make sure there are no hazards.

WORK-RELATED INJURIES

Basic steps to prevent injuries:

- Get help.
- Wear safety equipment if needed.
- Get a good grip.
- Stand close to the object.
- Tighten abdominal muscles and lift gradually.

What do I do if I have a work-related injury?

- Report the accident to your supervisor.
- Go to Employee Health (during administrative hours) or the Emergency Department (during WHEN hours) with your supervisor.
- Use ASISTS to complete VA Form 2162 (Report of Incident) and OSHA Forms CA-1 or CA-2. ASISTS (Automated Safety Incident Surveillance Tracking System) is a VISTA computer program to record all work-related injuries and illnesses.

Reporting the accident to your supervisor:

- Is required.
- Facilitates processing your injury/illness, especially if compensation is desired.

Employees need ASISTS:

- If an employee files for compensation for their injury/illness, they must complete a CA-1 or CA-2 in ASISTS.
- Help is available to fill out the CA-1 or CA-2.

Supervisors need ASISTS:

- Every injury/illness **MUST** be reported in ASISTS.
- Supervisors **MUST** complete and electronically sign the VA Form 2162 (Report of Incident) within two days.
- If compensation is filed for, the supervisor must complete and electronically sign the supervisor part of the CA-1 or CA-2 within three days after the employee has signed.

If you return to work on light duty due to a job-related injury:

- You must provide medical documentation to your supervisor stating specific restrictions to duty, using Form OWCP-5, and the length of time those restrictions apply.
- You must be cleared by your treating physician before you can return to full duty.

If you are unable to return to duty due to a job-related injury:

- You must provide medical documentation to your supervisor that states “due to a job-related injury, you are totally disabled and you are unable to perform any duties” and the length of time that this applies. This documentation must be provided within 10 working days.
- Continuation of Pay (COP) will not be authorized without this documentation.

Following these procedures will help you avoid delays with the processing of an Office of Worker’s Compensation (OWCP) claim.

SMOKING POLICY

There is **NO SMOKING** allowed inside any building on the premises of NYHHS or near entrances or exits.

An individual should not have to pass through second-hand smoke to enter or exit a building. This means you cannot stand in front of an exit and smoke.

Smoking shelters are available:

- NY campus: One shelter by the security gate and the entrance of the courtyard
- BK campus: One shelter at the rear entrance of Building 1
- SA campus: Two shelters outside Building 89 and one by the Outpatient Clinic (Building 88)

UTILITIES SYSTEMS

Utilities are defined as critical building systems and are managed by Engineering Service. Various types of utilities include:

- Heat
- Elevators
- Water
- Air conditioning
- Plumbing
- Medical gases
- Steam
- Electricity

You should become familiar with the utilities in your area. Two important concerns are emergency power and medical gas.

EMERGENCY POWER

You should know where emergency powered outlets are in your area. Most outlets on emergency power are either colored red or labeled "emergency power." However, in some locations, the entire area has emergency power.

MEDICAL GAS

If you work in an area supplied by medical gas, you should know:

- Who is responsible for shutting off the gas
- What to do in the event of a medical gas panel alarm

If you are responsible for shutting off the gas, you should know:

- Which shut off valves go to each area
- How to shut them off
- Emergency procedures for maintaining patient care

CONTACT INFORMATION

If a utility fails during the day, call Engineering:

- NY: Call ext. 3000
- BK: Call ext. 3000
- SA: Call ext. 2355

If a utility fails during a weekend, holiday, evening or night shift (WHEN hours):

- NY: Notify the night engineer
- BK: Call ext. 3597
- SA: Call ext. 2689

These numbers appear on the red tag on your ID badge.

CONTINGENCY PLAN

Your service should have written contingency plans that describe what to do in the event of all types of utility failures. These plans can be found in your RED Emergency Management Manual.

EMERGENCY MANAGEMENT

EMERGENCY MANAGEMENT MANUAL

The Emergency Management Manual (the RED book) contains four sections:

1. Introduction – Contains the purpose, mission statement, definitions and general employee responsibilities.
2. Response and Recovery Plan – Contains the emergency operations plan, the emergency operations center data, the NYHHS HEICS plan and assigned incident command roles and job action sheets and various plans and policies relating to Emergency Management.
3. National Disaster Plan – Contains the VA/DoD contingency plan and the Disaster Emergency Medical Personnel System (DEMPS) policy.
4. Service-Specific Section – contains policies and plans relating to your service.

FOUR PHASES OF EMERGENCY MANAGEMENT

1. Preparedness – Plans and preparations before an emergency or disaster occurs, for example the Emergency Management Manual, drills and exercises and training
2. Response – Actions taken during an emergency or disaster for the purpose of reducing casualties, limiting property damage or harm to the community; response is putting your preparedness plans into action
3. Recovery – Actions taken to return to a normal or even safer situation following an emergency or disaster, for instance, rebuilding or repairing damage
4. Mitigation – Activities that prevent an emergency, reduce the chance of an emergency happening or reduce the damaging effect of an unavoidable emergency. Mitigation takes place both before and after an emergency. Stockpiling medication is an example of mitigation.

HOSPITAL EMERGENCY INCIDENT COMMAND SYSTEM (HEICS)

HEICS is the incident command system that has been adopted by NYHHS. HEICS requires incidents be managed by an Incident Commander (IC). The IC is supported by a command structure as outlined in the Emergency Management Manual. HEICS is used for all emergency management plan activities, drills and exercises. The IC and the key staff and the Emergency Operations Center (EOC) use HEICS to ensure that a proper chain of command is followed and that all efforts are coordinated.

WHAT TO DO DURING AN EMERGENCY PLAN ACTIVATION

- Follow the general employee responsibilities.
- Follow your service-specific plan.
- Report to the labor pool as needed.
- Follow the directions of HEICS command staff.

DISASTER EMERGENCY MEDICAL PERSONNEL SYSTEM (DEMPS)

The VA has a nationwide register of personnel who volunteer their special skills in response to emergencies. This register is used to provide personnel to serve for a limited time period as disaster workers. DEMPS is a completely volunteer program. NYHHS accepts volunteer applications for DEMPS.

DECON TEAM

Any employee may volunteer to be a Decon Team member. Training to the Hazardous Materials Operations Level is provided. The Decon Team drills monthly at the BK and NY campuses.

SECURITY MANAGEMENT

ID BADGES AND FINGERPRINTING

ID badges must be visibly worn by all employees and trainees at all times. New employees including consultants and other intermittent staff as well as contract personnel and trainees must be fingerprinted by Human Resources Management Service prior to receiving their ID badge. Fingerprint information is sent directly to the federal government's Office of Personnel Management. If you lose your ID badge or have it stolen, contact the Police and Security Service to make arrangements for obtaining a new badge.

VEHICLE REGISTRATION

All staff must register their vehicles with the Police and Security Service.

STOLEN PROPERTY

If you discover that a personal or government-owned item is missing or stolen, report it to your supervisor and then to the Police and Security Service, which will investigate the report. The Police and Security Service tracks thefts and reports on trends to the Environment of Care Committee. CBOC (community based outpatient clinic) staff are to report stolen personal property to local authorities.

INFORMATION SECURITY

The Information Security Officer (ISO) is automatically informed when you access data on yourself or another employee or trainee in the computer. You should not view data on anyone unless it is job related. See the section on Information Security for additional information.

CONTRABAND

Drugs, alcohol and weapons are contraband. It is illegal to bring contraband onto VA premises. If you see contraband items report these to Police and Security Service.

VIOLENCE

Get help when dealing with violent patients. If you witness uncontrolled or violent behavior, dial 2000. The Code 2000 psychiatric intervention team is trained to respond to behavioral emergencies. CBOC staff should use 911.

Protect yourself. Be aware of your surroundings. Leave work whenever possible with a co-worker. Have your keys ready when leaving work and approaching your vehicle. Stay in well-lit areas. Always secure your office and personal items.

See the section on Workplace Violence Awareness and Prevention for additional information.

WORKPLACE VIOLENCE AWARENESS & PREVENTION

NYHHS affirms that employees should work in environments free from attack, threats and menacing and harassing behaviors.

THE FACTS

- One in every six violent crimes currently committed in the United States happens at work.
- Each year, nearly two million people are victims of violent crimes which are mostly aggravated assaults while on the job.
- According to the National Institute for Occupational Safety and Health, each week an average of 20 people are killed and 18,000 people are assaulted while working or on duty.
- Homicide is the no. 1 cause of death of women in the workplace and the second leading cause of death of men in the workplace.
- Workplace homicides have increased tenfold over the last decade, with murders accounting for 17 percent of all workplace deaths.

WARNING SIGNS AND TRIGGERS

Workplace violence may include damage to property, serious harm, injury or death. Warning signs are apparent in two-thirds of cases and should not be ignored.

Potential employee “triggers”--red flags that lead up to an incident of workplace violence--include:

- Decreased productivity, inconsistent work patterns, concentration problems
- Increased lateness and/or absenteeism
- Depression and social withdrawal
- Decreased attention to appearance and hygiene
- Difficulty relating to co-workers
- Threats or verbal abuse of co-workers and supervisors
- Challenges to authority; resistance and overreactions to changes in procedures
- Explosive outbursts of anger or rage without provocation
- Preoccupation with firearms and other dangerous weapons

Each of the above behaviors is a clear sign that something is wrong and that the employee needs appropriate supportive interventions. Supervisory behaviors that foster good communication and mutual respect are essential in helping to create a positive work environment.

Workplace violence is more likely to occur during “employment junctures” than at other times. These are situations in which there is a major change in an employee’s status or perceived status that will be looked on as negative. The most common types of employment junctures are:

- Disciplinary actions
- Involuntary job reassignment or transfer, layoff or termination
- Workplace deterioration, such as more assigned duties or uncertain job security

TAKING ACTION – WHAT YOU CAN DO

- Wear ID badges according to VA policy.
- Assess your workplace regularly to see where violence might occur.
- Identify and report unsafe areas and hazards.
- Be alert for potential violence and suspicious behavior and report it to your supervisor and Police Service.
- Assess patients for their potential for violence and alert colleagues about patients with known histories of assaultive behavior; maintain confidentiality but alert staff accordingly.
- Report and document assaults, verbal abuse and incidents of feeling threatened by anyone.
- Be supportive of those who encounter workplace violence. Make sure they receive necessary treatment and counseling.
- Review NYHHS’s security procedures in the Emergency Preparedness Manual. Policies with additional information are: Response to Violence in the Workplace (No. 07B-10), Violent Behavior Prevention Program (No. 00-27) and Prevention and Management of Suicidal and Assaultive Patients (No. 11M-2).
- Attend training on preventing or defusing violent situations, dealing with conflict and stress management.
- IF YOU WITNESS UNCONTROLLED OR VIOLENT BEHAVIOR, CALL CODE 2000.

OCCUPATIONAL HEALTH

Occupational Health provides services for:

- Pre-employment/placement examinations
- Clearances for specific position descriptions
- Medical surveillance (in accordance with VA Directive 5019, OSHA, NFPA, and other regulatory agencies)
- On-the-job injury/illness and necessary follow-up
- ONE TIME ONLY evaluations for non-work related injury/illness:
 - To alleviate discomfort
 - To keep the employee on duty for the remainder of that tour

Employees are responsible for complying with NYHHS policies regarding:

- Infection control
- Medical surveillance
- Health maintenance

Occupational Health:

- Promotes a healthy workplace
- Protects employees, co-workers and patients
- Helps everyone benefit when all employees comply with required medical surveillance

It is the policy of NYHHS to ensure a hazard-free work environment for employees, as follows:

- Compliance with the TB control program is considered a condition of employment at this facility.
- Occupational Health is available at either campus to administer and read a PPD test.
- An employee who fails to comply may be sent off duty on LWOP status until a test is completed.
- Exposure to any body fluid(s) or other potentially infectious material must be reported to Occupational Health or to the Medical Officer of the Day (MOD) IMMEDIATELY.

Occupational Health records are CONFIDENTIAL.

- Only authorized staff members may view them.
- Employees must have written authorization to view their own records.
- Written authorization is also called a "Release of Information."

When assigned to Occupational Health or Urgent Care:

- A provider may order diagnostic labs or medications for the emergency management of illnesses and injuries (e.g., an on-the-job injury, sick call).
- Medical providers CANNOT order diagnostic labs or medications for their co-workers/colleagues outside these parameters.
- A progress note titled "Occupational Health" will provide justification for any corresponding orders.
- Eligible employees (veteran status) may receive ongoing routine treatment of medical conditions through their VA primary care provider.

When an employee suffers a serious non-work related illness during duty hours:

- An Urgent Care provider will render needed first-aid treatment.
- The employee will be referred to a private Emergency Room or private physician's office.
- The employee may be charged sick leave from the time they leave their duty station.

When an employee suffers an on-the-job injury:

- They will be evaluated by an Occupational Health provider, Urgent Care provider or MOD.
- They must be accompanied by their supervisor or designee.
- The medical provider will evaluate and recommend the job tasks the employee may perform.
- ONLY THE SUPERVISOR can authorize an employee to go off duty.
- Light duty assignments are available for employees with on-the-job Injuries who cannot return to work in a full duty status.
- The supervisor must complete VA Form 2162 in the ASISTS package in the VistA computer program.
- Employees with work-related injuries may choose either the VA or a private physician for any needed follow-up evaluations.

When the VA is chosen as the provider for an on-the-job injury:

- The employee must report to Occupational Health before and after each appointment, if referred for specialist care.

- All documentation and requests for further appointments must be approved by the Occupational Health physician.
- In this instance, the Provider of Record is the Occupational Health physician.

When an employee requests leave while on duty:

- They do not need to be referred to Occupational Health or to the MOD if they do not feel well and want to go home.
- They do not need to be referred to Occupational Health or to the MOD if they are going to see their personal physician.
- The supervisor should approve the request when the employee is clearly ill, and allow the employee to seek relief in an off-duty status.

Employees with non-work related injuries:

- Must seek any needed follow-up from private sources.
- VA follow-up may be provided to those employees who are eligible for care as veterans through their VA primary care provider.

When an employee reports to Occupational Health for sick call:

- Sick leave will be charged starting at the time an employee reports to Occupational Health or Urgent Care to seek medical attention.
- Occupational Health services for a NON-WORK RELATED illness/injury cannot be used as a routine health care provider.
- ONLY emergency care or ONE TIME TREATMENT may be provided through Occupational Health or the Urgent Care area.
- Light duty for non-work related injury/illness is not available, and will not be offered under any condition.
- Employees returning to work after an illness of three or more workdays may be evaluated in the Occupational Health clinic for clearance to return to duty at their supervisor's discretion.

ONLY Human Resources Management Service can request a fitness-for-duty exam.

- The supervisor must provide all the appropriate documentation to Human Resources Management Service.
- No fitness-for-duty examinations or evaluations will be performed by Occupational Health unless requested by Human Resources Management Service.

Occupational Health records are maintained on site for three years following an employee's termination of employment.

- Records are then forwarded to a repository in St. Louis, Missouri.
- Surveillance records are kept for the term of employment plus 30 years.

GEMS

GEMS (Green Environmental Management System) is a management tool to monitor and improve NYHHS's environmental performance and to help protect the health and safety of everyone at the facility and protect our community. GEMS is a group effort that goes beyond just environmental compliance. NYHHS has a GEMS Committee to oversee and coordinate the program. The policy for GEMS is 137-13 and can be found on the intranet.

GEMS' purpose is summed up in the VA's own environmental statement: The VA is committed to the health of the environment and promotes pollution prevention, energy efficiency, acquisition of environmentally preferable products and services and the "three R's" of waste prevention and management: Reduce, Reuse, Recycle.

REDUCE

- Conserve energy and reduce material usage – turn off lights and equipment when not in use and minimize material and water usage.
- Drive your car less by walking, biking, carpooling and using public transit.
- View documents on the screen instead of printing them out.
- E-mail someone instead of faxing them.
- Print or copy on both sides of the paper.

RECYCLE

- Recycle as much as possible – newspaper, office paper, glass, plastic, aluminum, ink cartridges and batteries.
- Soda bottles and cans
- Buy goods made from recycled materials
- Use solvent recycling equipment for lab solvents.

ENVIRONMENTAL LAWS AND THE GEMS PROGRAM

These are some of the laws the Environmental Protection Agency (EPA) has to protect our air, water and soil:

- Clean Air Act - Controlling air pollution from boilers, EtO sterilizers and other work activities
- Safe Drinking Water Act - Not pouring chemicals down the drain; preventing chemical spills and releases
- Resource Conservation and Recovery Act - Properly managing hazardous wastes generated from our work so they do not contaminate the environment

Do you use, dispose of and/or store paint, solvents, fluorescent light bulbs, computers, batteries, motor vehicles, aerosol sprays, solid waste, hazardous/radiological waste, large amounts of water or electricity, chemicals or medical supplies? If so, you could impact the environment by causing a spill or release of hazardous chemicals due to incorrect storage or disposal of waste that could pollute the air, water and/or soil.

GEMS IS EVERYONE'S RESPONSIBILITY

- Identify tasks/activities that can impact the environment (e.g., EtO sterilization and boiler operations, air emissions, medical-surgical wastes and lab analyses, chemical wastes)
- Conduct service-specific training on ways to reduce impacts (reduce wastes, use less energy, use recycled or re-usable products)
- Conduct service-level environmental rounds of work areas (ensure waste containers are kept closed, labeled and properly stored)

EXAMPLES OF WASTE STREAMS MANAGED BY GEMS

- **Solid Waste**
Paper, steel and aluminum cans, cardboard, plastics, bulky waste
- **Biohazardous Waste**
Blood/blood products
Pathological waste
Dialysis unit waste
Sharps
Cultures
- **Universal Waste**

Fluorescent bulbs from light fixtures, mercury lamps
Mercury-containing equipment (e.g., thermometers, sphygmomanometers and thermostats)
All batteries (from VA equipment only)
Used oil
Computer equipment

- **Hazardous Waste**
Oil paints, paint thinners
Toxic chemicals - acids, bases, organic solvents
Hazardous drugs - nicotine, chemotherapy
Compressed gases
Dental amalgam
Housekeeping cleaners and disinfectants

No matter what type of material is involved we should:

- Order only the quantity that's needed.
- Purchase the safest material for the job.
- Make sure that all items are properly labeled.
- Handle and store the material properly.
- Collect and properly recycle or dispose of the material when its no longer needed.

...and ensure that waste is handled correctly:

- All waste containers should remain closed at all times. They can only be opened while placing items inside!
- Incompatible wastes must be properly separated and stored in preparation for disposal.

GEMS also includes:

- Storm water discharge and other types of discharges or releases
- Air pollutants from boilers and emergency generators
- Underground storage tanks

GEMS is about energy conservation and buying green, a.k.a. green purchasing or affirmative procurement and pollution prevention. In short, GEMS is involved with anything that can have an impact on our environment.

Failure to comply with environmental requirements could result in:

- An unplanned spill or release that could pollute the air, water or soil.
- License revocation, costly fines or criminal charges.
- Bad publicity. White River Junction VA hospital was fined \$372,254 for improper handling of hazardous and sometimes potentially explosive materials and other waste issues.

GEMS is a never-ending process that involves continuous improvement. We review and modify our procedures to ensure compliance to current regulations and meet new environmental initiatives that target pollution prevention.

Finally, we can support GEMS by working to...

- Maintain regulatory compliance.
- Implement controls and train employees.
- Follow established procedures to prevent unplanned spills and releases.
- Ensure that sampling and monitoring devices are calibrated and operating correctly.
- Conserve energy and water.
- Use recycled products.
- Prevent pollution by substituting "green" products.

Need more information? Contact: Stephan Thomatos, NYHHS GEMS coordinator, ext. 4049, BK campus.

INFORMATION SECURITY AWARENESS

This training focuses on important security practices and procedures. It includes information that VA employees, contractors and volunteers must know in order to protect information about veterans that is stored on VA systems. The Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) requires that you complete this training. When you complete the course, you have met this training requirement.

OUTCOME OBJECTIVES

- Describe when to contact your Information Security Officer (ISO)
- List the elements found in a secure password
- Recognize confidential information
- List VA policies on how to protect information
- Express cyber security requirements to protect an individual's privacy
- Explain how to back up sensitive data
- Discuss the potential danger of using e-mail
- Discuss the potential danger of using a wireless network
- Restate how to report suspicious incidents to your ISO
- Describe how important VA information is to the government and veterans
- Differentiate between the use of VA information resources in your work setting versus for your personal use
- The Rules of Behavior for all VA employees

INTRODUCTION

- "Cyber Security Awareness" helps to protect VA computer systems and data. It is more than policies, procedures, rules and regulations. Cyber Security Awareness helps you understand what you need to do to ensure:
 - Confidentiality, integrity and appropriate availability of veterans' private data,
 - Timely and uninterrupted flow of information throughout VA systems,
 - The protection of VA information systems from fraud, waste and abuse
- If you suspect that VA information systems have been violated or put in danger (compromised), report this to your Information Security Officer (ISO).
- Much of what you learn in this course will not only help you protect VA information, it will also help protect you as a computer user.

KNOW YOUR INFORMATION SECURITY OFFICER (ISO)

Do you know the rules and requirements to keep VA's information secure? For example:

- Do you know what to do if your computer is infected with a virus?
- Do you know what to do if you see someone using VA computers for theft or fraud?
- Do you understand your role in protecting confidentiality and privacy?
- Are you sure that your work is backed up and safe?
- Do you know your role in your facility's contingency plan?

Every VA facility has an ISO. He or she can help you answer these questions. He or she also can help you understand your responsibilities.

- NYHHS's Information Security Officer is Joan Rodriguez. She may be reached at the BK campus, ext. 4064.
- Alternate Information Security Officers: Judy Ortiz – BK/SA campus; Ernie Coon – NY campus; Pam Roehrl – CBOCs.

PASSWORDS

- Passwords are important tools for protecting VA information systems and getting your job done. They ensure that you--and only you--have access to the information you need.
- Keep your password secret.
- If you have several passwords, store them in a safe and secure place that no one else knows about.

Password Requirements

Passwords must:

- Have at least eight characters (i.e., Gabc123&).

- Use at least three of the following four kinds of characters:
 - Uppercase letters (ABC...)
 - Lowercase letters (...xyz)
 - Numbers (0123456789)
 - "Special characters," such as #, &, * or @
- Be changed at least every 90 days.

Using these rules will provide you with a "strong" password. VA requires strong passwords on all information systems.

Rules of Thumb for Passwords

- Don't use words found in a dictionary.
- Follow the rules for strong passwords.
- Don't use personal references (names, birthdays, addresses, etc.).
- Change your passwords at least every 90 days. If you suspect that someone may know your password, change it immediately and inform your ISO.
- Never let anyone stand near you while you type your password. Ask people to turn away while you type it and don't let them see your keyboard while you type.
- If you have several passwords to remember, write them down. But, keep them in a locked place so that no one else can get to them.

Summary

The most common way to access VA systems and computers is by entering the correct username and password. Your username and password protect you and the information stored on VA computers.

Do not tell anyone your username or password. If you do, then you no longer control how your password and username can be used.

If someone else uses your account information, you are responsible. Usernames are easy to get because they are based on people's names. This is a necessary risk. That's also why it's important to create a strong password—and keep it a secret.

CONFIDENTIALITY

"Confidentiality" at VA means information is available only to those people who need it to do their jobs. At VA, confidentiality is a must. VA computers are set up to protect confidentiality. But you also have to do your part.

Maintaining Confidentiality

- Do read and follow remote access security policies.
- Do not walk away from a computer without logging off.
- Do not print private data and leave it on the printer.
- Do access information systems only through approved hardware, software, solutions and connections.
- Do take appropriate steps to protect information, network access, passwords and equipment.
- Do control access to patient files or data saved on a disk.
- Do not access information you don't really need.
- Do avoid using automatic password-saving features.
- Do not talk about a veteran's case in a public place.
- Do promptly report any misuse of the remote access process or report if private information has been compromised.

Media Destruction and Confidentiality

How would you feel if your personal information was stored on a computer and then that computer was given to another person? That would be a breach of your confidentiality and you wouldn't like it. But this has happened before at VA.

- One of the jobs of Information Technology (IT) staff is to get rid of old computer equipment.
- VA has a media destruction contract that destroys anything that holds electronic data (drives, tapes, memory sticks, etc.). Electronic data are destroyed using the same process—no matter what size, shape, or form.
- You can help reduce the risk of private information falling into the wrong hands.
- When possible, store data on network drives—not your desktop computer.
- If you see computers being excessed without full data erasure, let your ISO know.
- Remember that clicking on the delete button doesn't really delete everything from your computer.
- Follow your local policies and procedures for disposing of printed copies of sensitive information.
- Contact your ISO for media destruction procedures.

Backups

Any work you do on VA's computers is important. It is important to you because of the time and effort expended to create it. It is important to VA and to veterans because it supports our mission. There are some resources that we can't afford to lose, so database backups are systematically and routinely created on systems such as Vista, BDN and others. Backups are cheap insurance. The question is not **if** you will ever need to use your backup—the question is **when**; so making backups is a smart practice for your home computer, too.

- Staff at NYHHS are instructed to place ALL data files on the Network drive, which is automatically backed up each night. There should be NO DATA on the machine's hard drive (C:), since the machine itself is not backed up.
- Your facility's network is the best place to create a backup. If your work has sensitive data in it, make sure the file is password protected so only you can get to it. Paper files with patient-sensitive information should be locked away from others.
- Backups containing sensitive data must be securely stored. You should be sure to lock information in a secure area if it contains sensitive data. Employees who transport, transmit, access, use, process, or store VA Protected Information outside VA facilities (even one time) are responsible for requesting and obtaining supervisor and ISO approval in advance.
- Check with your ISO or IT staff. They can help you create a way to routinely back up your data.

Summary

VA information technology staff work hard to make sure the VA network is safe and routinely backed up. But they cannot protect files that are not stored on the network. It is your job to make sure that all data is saved to the Network Drive and that there is no data stored on the local, or C: drive.

E-MAIL

Electronic mail (e-mail) helps us do our jobs faster. But using e-mail also has risks.

E-mail Privacy and Security

- E-mail isn't like a personal letter delivered to you in a sealed envelope by the post office. Instead, e-mail is more like a postcard that gets dependably delivered, with opportunities along the way for other people to see what it says.
- E-mail is not private. Never use e-mail to send private information about veterans or employees unless it is encrypted. Like any other e-mail system, the VA network is at risk for virus attacks. Most computer viruses are spread by e-mail.

Chain Letters and Hoaxes

- Chain letters and hoax messages slow down the VA network. Never forward these messages to others. In fact, it's best that you delete the message without opening it.
- Also, never reply by saying, "Please stop." It slows down the VA e-mail system.

E-mail Safety Hints for Work and Home

- Use virus protection software and keep it up to date.
- Make sure your virus protection program scans all e-mails and attachments that are sent to you and also scans the messages you send.
- Learn to recognize the signs of a virus infection.
- Don't expect privacy when using e-mail to transmit, store and communicate information.
- Always be cautious when opening e-mail from people you don't know. Make sure the subject line is appropriate before opening the message. If you are not sure, then don't open the message.
- Don't open attachments from senders you don't know.
- Don't forward or create hoaxes or ask people to modify their computer systems.
- Don't spread rumors using e-mail. Be suspicious of any message that tells you to forward it to others.
- Don't participate in "mail-storms." Don't send a message that says "me too" or "thanks" or "please stop."
- Use "Reply to All" sparingly. Does everyone in your large e-mail group really need to see your response? Often, it's more appropriate to limit your response to just the sender.
- Replying to unsolicited spam e-mail is actually more likely to increase the number of messages sent to your address. When spammers receive a reply, the reply tells them your e-mail address is valid.
- If you have to e-mail private or personal information about a veteran or VA employee, you are required to encrypt the message (put it into code). Most cryptographic systems make sure the message is valid. They also help prevent someone else from reading or tampering with the message.
- If you have any questions about how to deal with spam or how to encrypt a message, talk to your ISO.

Remote Access

On June 7, 2006, VA issued a new policy (VA Directive 6504) about using, accessing and sending VA data while outside of VA facilities. You are only allowed to access, use or send VA data while offsite if you have the permission

of your supervisor. Also, you can only do so when appropriate security steps have been taken. The policy states that:

- You can only access, use or send VA information from a VA-owned laptop, handheld computer or storage device. You cannot use your home computer, personal laptop, or storage device to access, use or send VA data.
- You must have your supervisor's permission.
- You must apply for this permission through your ISO.
- You cannot share VA information with anyone else.
- You must not share your username or password—or instructions on how to access the VA network—with anyone else.
- You cannot store VA data on your personal computer or laptop.

If you believe this policy has been violated, report the violation to your ISO as soon as possible.

Wireless Network Security

If you use a wireless network, it is important that you know how to use it safely—and know the potential consequences if you don't. Wireless networks, which use radio waves to transmit data, are being used more often all the time by federal agencies. They allow users to do their work while moving around from one location to another. But wireless networks are just as vulnerable to attacks by hackers, viruses and other threats as traditional computers. Poorly controlled wireless networks can allow sensitive data, passwords and other information to be read, changed or transmitted by unauthorized users.

Here are some examples of the dangers associated with wireless networks:

- Another person can eavesdrop on a transmission between two workstations (e.g., a wireless handset and a base station).
- An attacker can analyze traffic to learn more about an organization's communication patterns, such as set days or times that personal information is sent from one employee to another.
- An attacker can pretend to be you to get access to private information, to change data or to send it to someone else.
- An attacker can become "the man in the middle" by intercepting messages, stopping them from being sent or transmitting them to someone else.
- An attacker can change or delete a message.
- An attacker can jam a wireless network with extra radio signals to stop you from accessing information. Other devices such as cordless phones or microwaves can prevent a wireless network from working properly.
- If you use a wireless network, contact your ISO to learn more about how you can do your work safely.

VIRUSES

High-tech vandals have created dangerous programs that have infected VA systems. When this happens, it's more difficult to do our jobs. It takes time and money to defend against viruses. But you can take an active role in virus defense by:

- Making sure the computer you use is protected and up to date.
- Letting antivirus programs run until they are complete.
- Not opening e-mail attachments from people you don't know.
- Looking for the signs of virus infection, such as when your hard drive is constantly active.
- Making sure data files and programs on your computer are authorized, scanned and virus-free.

Anti-Virus Program

VA uses a Department-wide antivirus program. Often, antivirus software is automatically installed and updated. But new viruses are developed every day. They can be spread from inside or outside VA. There is no protection from newly discovered viruses. That's why it is important for you to protect yourself—and VA.

Worms and Trojan Horses

Worms and Trojan horses are software programs created for one main purpose—to stop computers or networks from working properly. These types of threats are known as "malware." A Trojan horse can carry a virus or worm. Here are some basic definitions for the types of malware and how they impact your system:

- A virus is a software program that is loaded onto your computer and executed without you knowing it. Viruses can be spread in many ways—from a diskette, CD-ROM, DVD, removable storage devices (such as Zip drives) or e-mail.
 - One type of virus is called a worm. Worms can replicate themselves. It is easy to produce a simple virus that can make a copy of itself over and over again. A worm can be dangerous because it quickly uses all of the available memory on your system and brings it to a halt. Viruses

that can get around VA protections and attack one computer after another are even more dangerous.

- Another type of virus is a Trojan horse. This term comes from a story in Homer's Iliad. The ancient Greeks gave a giant wooden horse to their enemies, the Trojans, as a peace offering. After the horse was moved inside Troy's city walls, Greek soldiers snuck out of the horse's empty belly and opened the city gates. This allowed more soldiers to enter Troy and destroy it.
- These programs may seem harmless. Even though they do not replicate themselves, they can be just as destructive as viruses and worms. Their mission is to get destructive viruses into computers and networks. One of the worst Trojan horse programs claims to rid your computer of viruses, but it instead introduces viruses onto your computer.
- Malicious e-mail hoaxes are not viruses but they can still be dangerous. In most cases, the sender asks you to forward a warning message to everyone you know. A good example of an e-mail hoax is one that has a subject line that says, "Delete this file immediately." The message tells you how to locate a computer file and delete it. A hoax may offer a way to help you fix a problem, but when you do what it asks, it actually disables your system.
- Even messages that are harmless can still cause problems. When these messages are forwarded to others, this action slows down the VA network, which also slows down the process of serving America's veterans.

Symptoms and Virus Defense for Work and Home

There may be a problem if your computer has any of these symptoms:

- Reacts slower than usual
- Stops running for no apparent reason
- Fails to start ("boot")
- Seems to be missing important files
- Prevents you from saving your work

Virus Defense for Work and Home

- All VA computers must have virus protection software. To work properly, virus protection must be kept up to date. New updates are usually issued nearly every day.
- Contact your ISO or information technology staff if your VA computer is not up to date. While many sites automatically update virus protection software on network computers, some systems are not updated automatically. It is critical that you update your antivirus protection regularly.

Here Are a Few Tips:

- Delete e-mail messages from unknown senders or messages with unusual subject lines, such as "Open this immediately."
- Never stop or disable your antivirus program.
- Never stop your antivirus program while it's running.
- Back up your files on a regular schedule.
- Set your virus protection software to scan your e-mails and attachments.
- Be very careful if someone sends you an attachment that contains executable code. You can recognize these by the file extensions, such as .exe, .vbs, .js, .jse, .wsf, .vbe and .wsh.
- Do not delete any system files when asked to do so in an e-mail.
- To learn more about computer viruses and your role in virus defense, talk to your ISO.

PUBLIC PEER-TO-PEER FILE SHARING

- Public peer-to-peer file sharing (commonly known as "P2P") refers to programs that let anonymous files be shared between computers. There are times when using P2P is helpful. But most of the time, these programs break the law by sharing copyrighted music, videos and games. Some common public P2P programs are Kazaa, Freewire, Grokster and Morpheus.
- P2P is not allowed at VA.
- P2P programs also can be used to spread viruses and "spyware." Spyware tracks what you do on your computer and send that information to thieves and hackers—without you even knowing it. For example, someone could use spyware to get information about you, your coworkers, veterans and veterans' families.
- This information could be used to steal your identity, buy items on a veteran's credit card, or collect personal financial information about a VA employee. In addition, P2P file-sharing makes the VA network run slower.
- Don't be a victim. Use your computer wisely. If you think your computer may have P2P software or spyware, tell your ISO.

INCIDENTS

You know how important computers are when we are doing our jobs. At VA, so much of what we do depends on our computers. Sadly, the same computers that help us serve veterans can be used for theft and fraud. Viruses can

attack our computers. Computers can be stolen or vandalized. They can be used to provide private information to the wrong people. All of these are examples of computer-related incidents. It is important to tell your supervisor and ISO when you see such incidents.

Incident Do's and Don'ts

If you think a computer security incident has occurred, you should:

- Gather all the information you can about the incident so you can give as many details as possible to your ISO.
- Write down the date, time and location the incident took place as well as the computers that may have been affected.
- Tell your ISO what happened.
- Write down any error messages that showed up on your computer screen.
- Write down any web addresses, server names or IP addresses involved in the incident.
- You've probably heard about the theft of electronic information from a VA employee's home. The data included names, addresses and social security numbers of millions of veterans. This data breach violates our promise to veterans and puts them at risk for identity theft.
- So, when you suspect that an incident may have occurred it's very important that you tell your ISO immediately. Don't wait.
- It's best to contact your ISO in person or by telephone rather than by e-mail. You may not contact the media (radio, TV, newspapers) or anyone outside your VA facility.

The most common security threats can happen while you are doing routine tasks, such as copying, saving, changing, or deleting files. Even these kinds of simple tasks can do a lot of damage. It's easy to let your guard down when you are very busy or dealing with a heavy workload. Hackers depend on this, which is why they make threats look harmless. The best thing you can do to prevent a problem is to not take any chances. Learn everything you can about security threats. And if you think there may be a problem, contact your ISO immediately

VA CYBER SECURITY: PART OF INFRASTRUCTURE PROTECTION

VA's information systems are a major part of how we help veterans. They also affect our readiness to work with other federal agencies, such as the Departments of Defense, Health and Human Services and Homeland Security, during national emergencies. The FBI has warned all federal agencies that their systems and the information in those systems are potential targets for attacks. Now more than ever, the VA's systems and the information they contain must be available to serve our nation and its veterans. Please be careful. Don't do anything that might damage our information systems or data.

Summary

- The work we do at VA is an important part of our nation's security. As a result, hackers and other threats are more likely to attack VA information and systems.
- VA employees must do their part to prevent such attacks, learn everything they can about information security and take the right steps if a problem occurs.
- Report any incidents to your ISO immediately. If he or she is not available, contact your Alternate or Network ISO.
- Have you heard of "social engineering?" Social engineering happens when a person tries to gain your trust in order to get information and resources that he or she can use for harm. This is an important information security issue!
- If people ask you for private information or want to use your computer, make sure you know who they are and know that they really need access to the information on your computer.
- Also, make sure they have permission to get such information or access as part of their jobs. Dishonest "social engineers" look for chances to get your password or gain access to information about VA's patients, employees, or budget. We know you want to be helpful, but social engineers may try to take advantage of your kindness.
- One example of social engineering that hurt a VA facility was a phone call from someone claiming to be from "the phone company." The thief said he was testing lines and long distance circuits. The thief then asked an employee to dial a special code, which gave him access to a long distance service.
- This scam resulted in thousands of dollars worth of unauthorized calls being made at VA's expense.
- As we learn more about the tactics hackers use to get access to VA information and resources, hackers continue to look for new ways to get around our protections. In fact, they are likely to use social engineering tactics to get information and resources.
- Social engineers will rarely ask for private information directly. Instead, they will try to gain your trust and build a relationship with you. When they think they have your trust, they attack.
- You have to be diligent in protecting VA from the tactics of social engineers. You are our first line of defense.

AUTHORIZED USE

The American people, especially our veterans, expect us to protect their information. They also expect that we will not abuse or misuse the resources provided to us to accomplish our mission. As a VA employee, you may have the privilege of some "limited personal use" of certain government resources, such as computers, e-mail, Internet access and telephone/fax service. This benefit is available only when it:

- Does not interfere with official VA business.
- Is performed on the employee's "non-work" time.
- Involves no more than minimal expense to the government.
- Is legal and ethical.

Personal use of these benefits may be limited or eliminated at any time, especially if you abuse these privileges. To protect yourself, you should discuss your limits and responsibilities with your supervisor and ISO.

Ethics

According to information security author Winn Schwartau, "Ethics is about understanding how your actions affect other people, knowing what is right and wrong and taking personal responsibility for your actions." **Ethics** deals with putting a **value** on acts, based on whether they are **good** or **bad**. Every society has rules about whether some acts are ethical. The same thing is true when using a VA computer to access private information.

Misuse or Inappropriate Use

Examples of misuse or inappropriate use are:

- Any personal use that could slow down, delay, or disrupt government systems or equipment. These include continuous data streams, video, sound or other large files that may slow down the VA network.
- Using VA systems to get unauthorized access to other systems.
- Creating, copying or sending chain letters or other mass mailings—no matter what they're about.
- Activities that are illegal, inappropriate or offensive to fellow employees or the public. These include hate speech or material that ridicules others because of their race, creed, religion, color, sex, disability, national origin or sexual orientation.
- Creating, downloading, viewing, storing, copying or transmitting sexually explicit or sexually oriented materials.
- Creating, downloading, viewing, storing, copying or transmitting materials related to gambling, illegal weapons, terrorist activities or any other illegal or prohibited activities.
- Using government systems or equipment to make money, to get another job or do any business activity (for example, consulting for pay, sale or administration of business transactions, sale of goods or services).
- Fundraising, endorsing a product or service, lobbying or engaging in political activity.
- Posting Agency information to external newsgroups, bulletin boards or other public forums without permission. This includes any use that may make someone else think that the information came from a VA official (unless approval has been obtained), or uses that are at odds with the Agency's mission or position.
- Any use that could cost the government a lot of money.
- Accessing, using, copying or sending VA computer software or data, private information, or copyrighted or trademarked information without permission.
- Be sure to discuss your limits and responsibilities with your supervisor and ISO.

CUSTOMER SERVICE: SERVICE RECOVERY – A STANDARD OF EXCELLENCE

RULES OF FIRST-CLASS CUSTOMER SERVICE

- Always do it right the first time.
- Do it very, very right when things have gone wrong for the customer.
- Customers do not give you a third chance. They simply walk away and never come back and they tell others how bad you are.

WHAT IS SERVICE RECOVERY?

- Doing it very right the second time
- Turning a negative experience into a positive “memorable” one
- A systematic approach to proactively solicit veteran feedback
- Responding to complaints in a manner that creates loyalty

THE SERVICE RECOVERY PROCESS

- APOLOGIZE/ACKNOWLEDGE – Positive service recovery stories begin with some version of, “I’m sorry.”
- LISTEN, EMPATHIZE AND ASK OPEN-ENDED QUESTIONS – Listening is an active process; empathy shows you understand what the customer is saying and that you care. Asking open-ended questions helps you gain and keep control.
- RESOLVE – Fix the problem quickly and fairly. Develop and implement solutions; involve the customer in reaffirming a partnership and building trust.
- ATONE – Try to make amends or reparation for the customer’s satisfaction. “We will make every effort to correct the problem and offer you improved service...”
- FOLLOW UP – Confirm that what went wrong has been put right and that you care.
- KEEP YOUR PROMISES – Be realistic about when and what you can and cannot deliver.

TOP 10 SERVICE EXPECTATIONS

1. Being given progress reports if a problem cannot be solved immediately.
2. Being told about ways to prevent a future problem.
3. Being treated like a person, not an account number.
4. Being given useful alternatives if a problem cannot be solved.
5. Being told how long it will take to resolve a problem.
6. Being allowed to talk to someone in authority.
7. Being contacted promptly when a problem is resolved.
8. Knowing who to contact with a problem.
9. Receiving an explanation of how a problem happened.
10. Being called back when promised.

DIVERSITY IN THE WORKPLACE

WHAT MAKES EACH PERSON UNIQUE?

Many factors make each of us an individual:

- Appearance (gender, body size, skin color, hairstyle, clothing, etc.)
- Age
- Ethnicity, culture (customs, traditions, language, etc.) and family life (values, family size, etc.)
- Religious, spiritual and philosophical beliefs
- Income or social status
- Sexual preference
- Physical and mental abilities
- Life experiences
- Education

PEOPLE DIFFER IN MANY WAYS

For example, cultural background (including ethnicity) can influence the way people communicate through:

- Body language
- Listening
- Speaking
- Expressing opinions
- Working style

DIVERSITY CHALLENGES

- Getting used to differences
- Coordinating work styles
- Learning to communicate
- Developing flexibility
- Adapting to change
- Understanding disabilities

CELEBRATE DIVERSITY

Diversity is as natural as the air we breathe. It can add value in our personal and professional lives. It adds dimensions to our work teams, improves decision-making and increases employee morale, acceptance and productivity. Advancing diversity requires both a corporate and individual effort. Diversity has a positive influence on the organization and our customers. Continuously, we need to celebrate the diversity among us. Take pride in your own uniqueness and welcome others as individuals with special qualities. Enjoy your similarities and your differences.

SEXUAL HARASSMENT & THE DISCRIMINATION COMPLAINT PROCESS

OFFICE OF RESOLUTION MANAGEMENT (ORM) DISCRIMINATION COMPLAINT PROCEDURES

The Office of Resolution Management (ORM) provides Equal Employment Opportunity (EEO) complaint processing services within the Department of Veterans Affairs that include confidential counseling, mediation, investigation and procedural acceptability determinations. ORM ensures compliance relating to the implementation of final agency and appellate decisions. ORM issues final agency decisions on alleged breaches of EEO settlement agreements. Under the leadership of the Deputy Assistant Secretary for Resolution Management, ORM accomplishes these responsibilities through the headquarters office and a national network of 12 field offices and 11 satellite offices.

An employee, former employee or applicant for employment may file a formal EEO complaint if he or she believes that discrimination occurred on the basis of race, color, religion, sex, national origin, age (over 40), disability, reprisal for prior EEO activities or sexual orientation.

PROCESSING STAGES

Informal Stage

An individual (aggrieved) who believes that he or she has been discriminated against must initiate contact with an EEO Counselor within 45 calendar days of the date of the matter alleged to be discriminatory, or in the case of a personnel action, within 45 calendar days of the effective date of action. The aggrieved may seek EEO Counseling by calling 1-888-737-3361, or for the hearing impaired call 1-888-626-9008 – TDD.

An EEO Counselor will advise the aggrieved that he or she must elect to have their dispute(s) informally resolved through the agency's Alternative Dispute Resolution (ADR) procedure(s) where the agency agrees to offer ADR or pursue resolution through the EEO complaint process.

Formal Complaint Stage

A formal complaint must be submitted in writing, preferably on VA Form 4939, signed by the complainant, and submitted to the local ORM Field Office within 15 calendar days of receipt of the Notice of Right to File a Discrimination Complaint. The ORM Field Office will determine if the complaint is acceptable for processing.

Investigative Stage

If a complaint is accepted for investigation, an EEO Investigator will be assigned to the case. The investigator is authorized to take statements from witnesses under oath and gather pertinent documents and records. The investigator will assemble the file and prepare a report, which summarizes the evidence gathered.

Advisement of Rights

When the investigation is completed, the complainant will be provided a copy of the investigative file and advised that within 30 calendar days of receipt of the investigative file, he or she has the right to request either a hearing before the Equal Employment Opportunity Commission (EEOC), or a Final Agency Decision (FAD), followed by a Final Agency Action (FAA) from the Office of Employment Discrimination Complaint Adjudication (OEDCA), or an immediate FAD from OEDCA.

PREVENTION OF SEXUAL HARASSMENT POLICY

- The Department of Veterans Affairs has zero tolerance for sexual harassment in the workplace.
- Sexual harassment is a form of sex discrimination that is a violation of Section 703 of Title VII of the Civil Rights Act of 1964.
- Sexual harassment is unacceptable employee conduct in the workplace and will not be tolerated. All employees have the right to work in an environment free from sexual harassment.
- Sexual harassment is an offensive abuse of power. It is not necessarily about sex. Both males and females can be victimized by sexual harassment.
- Prevention is the key to elimination of sexual harassment in the workplace.

DEFINITION OF SEXUAL HARASSMENT

Sexual harassment is unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature when submission to such conduct is made either explicitly or implicitly as a term or condition of

employment, that unreasonably interferes with an individual's work performance or creates an intimidating, hostile or offensive work environment.

Sexual harassment is not limited to explicit demands for sexual favors. It also may include such action as:

- Sexually oriented verbal kidding, teasing or jokes
- Repeated sexual flirtations, advances or propositions
- Continued or repeated verbal abuse of a sexual nature
- Graphic or degrading comments about an individual or the individual's appearance
- Display of sexually suggestive objects or pictures
- Subtle pressure for sexual activity
- Physical contact such as patting, hugging, pinching or brushing against another's body

FORMS OF SEXUAL HARASSMENT

Sexual harassment can take a variety of forms. Three distinct categories of such claims are recognized:

1. Quid Pro Quo

Quid Pro Quo sexual harassment involves a manager or supervisor, that is, someone with supervisory authority, who can carry out a threat or promise. Sexual harassment occurs when sexual favors are sought in return for job security, benefits or opportunities. It can be in the form of a threat, such as "perform sexual favors or get fired" or "your job will become intolerable unless sexual favors are granted." Even if a supervisor does not follow through with any action, the threats alone may constitute a hostile work environment. Sexual harassment may also include rewarding an employee in return for sexual favors, such as giving cash awards, higher ratings or promotions.

2. Hostile Work Environment

Sexual harassment occurs when sexual comments or conduct unreasonably interfere with an individual's work performance or creates an intimidating, hostile or offensive work environment. A supervisor or co-worker may be responsible for this type of conduct or non-employee in certain circumstances. A hostile work environment is usually found where a general pattern of workplace behavior exists that is sexually oriented and severe or pervasive. It may also be established even if both males and females are subjected to the conduct, if the conduct affecting one gender is more egregious.

3. Sexual Favoritism

Sexual harassment occurs when a supervisor passes over otherwise qualified persons in order to convey employment opportunities or benefits to employees who submit to a supervisor's sexual advances or requests for sexual favors. An example of sexual favoritism is a male working under a particular supervisor who notices that only females who socialize with and date his male supervisor get choice travel assignments. When he approaches his supervisor about getting better travel assignments, the supervisor responds that the male employee "doesn't have the right kind of equipment" to warrant the choice assignments.

DEFINING SEXUAL HARASSMENT BEHAVIORS

Sexually oriented behavior has been found to include:

- Letters, telephone calls, magazines, pictures and objects of a sexual nature or content.
- Deliberate touching, brushing, cornering, pinching or leaning over a person.
- Suggestive looks, comments, gestures or whistles.
- Unwelcome pressure for dates or sexual favors
- Sexual jokes, teasing, remarks and questions
- Pervasive behavior is that which is widespread, common or repeated.
- Severe behavior is that which would be found to be objectionable to a "reasonable person" under similar circumstances.

Examples of Sexual Harassment

- Nonverbal:
 - Suggestive or insulting sounds
 - Leering or ogling
 - Whistling
 - Obscene gestures and obscene/graphic materials
- Verbal:
 - Sexual Innuendoes and sexual remarks
 - Insults, threats and sexual propositions
 - Humor and jokes about sex or gender-specific traits
- Physical:
 - Touching others

- Pinching
- Touching oneself
- Brushing the body
- Cornering
- Actual or attempted rape or assault

Definition of Terms

- LEERING — staring in general or at a particular part of the anatomy
- OGLING — looking up and down
- OBSCENE GESTURES — suggestive facial expressions or sexual gestures
- NON-VERBAL HARASSMENT CAN INCLUDE: - Following a person; giving personal gifts or “hanging around” a person
- CORNERING — blocking a person’s path
- TOUCHING — touching a person’s clothing, hair or body; hugging, kissing, patting or stroking
- BRUSHING — standing close to or brushing up against a person
- INSULTS — telling lies or spreading rumors about a person’s sex life
- SUGGESTIVE REMARKS — conversations about sexual fantasies, preferences or history

SEXUAL HARASSMENT PREVENTION

Prevention is the best tool for eliminating sexual harassment. Managers and supervisors must watch for the potential for harassment and take all necessary steps to prevent harassment from occurring. However, if it does occur, supervisors and managers must ensure that the harassment is eliminated in a prompt and effective manner, minimizing the effects on the victim to the extent possible.

Management’s Responsibilities

- Inform all employees that sexual harassment is prohibited.
- Provide a mechanism for dealing with sexual harassment complaints.
- Respond promptly to complaints of sexual harassment by conducting and/or asking for a thorough investigation.

Employee’s Responsibilities and Conduct

- Clearly inform those engaging in inappropriate sexually oriented behavior that you find it objectionable, unwelcome and will not continue to tolerate it. Don’t expect a supervisor or a co-worker to read your mind. Tell him/her how their conduct offends you.
- Seek assistance promptly if you are the target of or observe severe or repeated instances of behavior that you believe qualifies as sexual harassment.
- Document instances of alleged sexual harassment, date and time of the act, any persons present when the alleged incident occurred and a description of the action involved or the comments made.
- Title V, Code of Federal Regulations, Part 735, states that the maintenance of unusually high standards of honesty, integrity, impartiality, and conduct by government employees is essential to assure the proper performance of the government business and the maintenance of confidence by citizens in their government. The avoidance of misconduct on the part of government employees through informed judgment is indispensable to the maintenance of these standards. As a federal employee, you have a responsibility to avoid misconduct such as sexual harassment.
- Title 29,CFR, Chapter XVI, Part 1604, Section II, Item C, states that an employer is responsible for its acts and those of its agents and supervisory employees with respect to sexual harassment, regardless of whether the employer knew or should have known their occurrence. Item D states that an employer may rebut apparent liability for such acts by showing it took immediate and appropriate corrective action.
- The “what if they were here?” principle holds that if you have any doubts that your own conduct may be considered offensive, ask yourself if you would act in this manner if a person with whom you have a personal relationship (for example, a spouse) were observing.
- Unchecked sexual harassment can have less identifiable consequences on others in the workplace. Harassment that is either ignored or denied by supervisors or management can erode overall morale and productivity, not to mention exposing the organization to possible litigation and embarrassing press.

Preventive Measures for Supervisors

- Routinely educate employees about what constitutes unlawful harassment and distribute the Prevention of Sexual Harassment Healthcare System Policy, EEO-05.
- Post and discuss complaint procedures.
- Remind employees at staff meetings that sexual harassment in the workplace is prohibited.
- Ensure that employees have received the EEO mandatory training on the prevention of sexual harassment.
- Address behaviors that might lead to allegations of sexual harassment immediately.

Preventive Measures for Everyone

- Some executives have concluded that they cannot even compliment their secretary on their attire without risking a charge of sexual harassment. As a general rule, the courts are not saying you cannot compliment a person, only that you need to be sure that the compliment will not offend that person or be misinterpreted by a third party who hears your conversation. If there is any hint that the person resents the compliment or any attention to her (or his) appearance, by all means choose your words carefully and/or take appropriate actions to include an apology, if necessary.
- The law was intended to protect individuals from sexual harassment, not as an option for solving every workplace dispute. The conduct must substantially affect the work environment of a "reasonable person" to be considered harassment. Unless the conduct is severe, a single incident or remark does not generally create a hostile environment. However, a single touching may be sufficient if it is particularly egregious.

Warning Signs of Sexual Harassment

- The display of sexually oriented pictures, objects or written materials in office areas and on computers, both as search materials and screen savers
- Frequent jokes or statements in the workplace of a sexual nature.
- Open use of sexual innuendo or pressure for dates.
- Routine occurrences of sexually oriented profanity.

Potential Victims of Sexual Harassment

- Your co-worker or supervisor asks you out on a date. Although you refuse, the co-worker or supervisor continues to ask.
- Your co-worker starts each day with a sexual remark or a dirty joke. Your co-worker insists these are innocent comments but you find them objectionable.
- It seems that you cannot go in and out of the work area without being touched.
- When you come to work, your co-worker constantly eyes you up and down in a suggestive manner, which makes you feel very uncomfortable.
- Your manager or supervisor told you it would be good for your career if you went out with him or her.
- In the place where you work, there are nude pictures or partially dressed models displayed, and these pictures offend you.
- Your co-worker gives you sexually suggestive looks or makes gestures of sexual nature.
- Your co-worker asks you to have sex with him or her. You refuse. You have now found out that your co-worker is spreading rumors and gossip about you.
- While at work, your co-worker frequently massages your shoulders, grabs your waist and places an arm around you.
- Your co-worker has made many attempts to kiss you on the lips or cheek. Although you have resisted these advances, your co-worker has continued this conduct towards you.
- When you are at work, your co-worker and supervisor refer to you as sweetheart, honey, baby or sweet thing. Although you requested that they refer to you by your name, they ignored your request.
- It seems that your co-worker cannot walk near you without having to brush up against you.
- When you are at work, your co-worker asks you when are you going to spend some time with him/her and suggests that you need a drink after work to relax.

EFFECTS AND CONSEQUENCES OF SEXUAL HARASSMENT

- On the victim:
 - Mental anguish and stress
 - Uncomfortable working environment
 - Impact on productivity and efficiency
- On the organization:
 - Loss of morale, productivity and efficiency
 - Increased absenteeism and turnover
 - Uncomfortable work environment
 - Adverse publicity
- On the offender:
 - Written counseling
 - Disciplinary/adverse action such as admonishment, reprimand, suspension or removal
 - Potential liability such as payment of civil suit damages and criminal prosecution (on a case-by-case basis)

HOW TO REPORT AN ALLEGATION OF SEXUAL HARASSMENT

- If the alleged harasser is your supervisor, tell the next higher manager.
- Report the incident to Denise Hinton, EEO Specialist, at 212-951-3352; or

- Call the Office of Resolution Management (ORM) at 1-888-737-3361; or
- Report the incident immediately to your supervisor.
- Report the incident to your local Federal Women's Program Manager.

Reasonable Person Standard

Trying to pinpoint what a hypothetical "reasonable person" would find objectionable is not a scientifically precise process. What it really amounts to is an effort to identify behavior that most people in the community would likely consider to be inside or outside the bounds of proper behavior under the same circumstances. The EEOC has emphasized that "the reasonable person standard should consider the victim's perspective and not stereotyped notions of acceptable behaviors." The reasonable person is one with the perspective of the victim. Thus, investigators should consider whether a reasonable person in the victim's circumstances would have found the alleged behavior to be hostile or abusive.

MYTHS AND REALITY

- **Myth:** Some people are under the mistaken impression that women in the workplace never harass men.
Reality: In fact, about 21 % of the harassment cases filed within the Department of Veterans Affairs involved women who are alleged to have harassed men.
- **Myth:** If you ignore sexual harassment it will go away. **Reality:** Some harassers regard a victim's attempt to ignore an incident as a sign of encouragement. In one survey, while 29% of victims said it "made things better" when they ignored sexual harassment, 61% said that telling a person to "stop" was more effective.
- **Myth:** Most sexual harassment involves a manager or supervisor harassing a subordinate employee.
Reality: The majority of sexual harassment complaints are based on the behavior of coworkers.
- **Myth:** Sexual harassment exists primarily in the "eye of the beholder." Almost any work or deed, no matter how innocent, can be labeled sexual harassment. **Reality:** Both the courts and the EEOC have adopted the "reasonable person" standard for evaluating behavior. Sexual harassment complaints based on isolated incidents and actions or words that are not unlikely to be found objectionable by a "reasonable person" are subject to dismissal.

DOES THIS INCIDENT INVOLVE SEXUAL HARASSMENT?

A representative of a hospital supply vendor routinely visits the Procurement Office. This "rep" considers himself a "ladies man" and always makes suggestive remarks to the two female clerks in the office. He addresses them as "sweetie" and "honey," and comments on their appearance with specific references to parts of their anatomy. At the end of each visit, he always asks the unmarried clerk for a date, and leaves her his personal phone number written on his business card.

The clerk repeatedly turns down his request for dates and tries to refuse the phone number, but the rep always forces the issue. Fearful of creating bad feelings, the clerk takes the business card, smiles politely and promises to "think about it." This clerk is very uncomfortable with the man's behavior and confides her feelings to the other clerk. The second clerk tells the supervisor that both women find the rep's behavior objectionable. The supervisor responds, "Yeah, he's a real smooth talker. But he's just trying to be friendly to his customers. Ignore him and he probably won't bother you." Shortly thereafter, the unmarried clerk contacts an EEO Counselor with a complaint of sexual harassment.

Is this sexual harassment? If your answer is yes, you have answered correctly. The vendor's behavior is deliberate, repeated and unsolicited. The vendor verbally harassed the unmarried clerk with terms of endearment and suggestive comments. He continues to ask her out, even though she has turned him down repeatedly.

NO FEAR ACT

NO FEAR ACT NOTICE

Congress enacted the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 on May 15, 2002. This act requires VA to comply with anti-discrimination and whistleblower protection laws. Congress found that federal agencies cannot operate effectively if those agencies practice or tolerate discrimination.

The act requires VA to provide this notice to all employees, former employees and applicants for VA employment to inform them of rights and protections available under federal anti-discrimination, whistleblower protection and retaliation laws.

ANTI-DISCRIMINATION LAWS

VA does not discriminate against employees or applicants with respect to the terms, conditions or privileges of employment on the basis of race, color, religion, sex, national origin, age, disability, marital status or political affiliation. Discrimination on these bases is prohibited by several statutes.

If you believe that you have been the victim of unlawful discrimination on the basis of race, color, religion, sex, national origin or disability, you must contact an ORM (Office of Resolution Management) Equal Employment Opportunity (EEO) counselor at 1-888-RES-EEO1, TDD 1-888-626-9008, within 45 calendar days of the alleged discriminatory action or, in the case of a personnel action, within 45 days of the effective date of the action.

If you allege discrimination based on marital status or political affiliation, you may file a written complaint with the U.S. Office of Special Counsel (OSC). As an alternative you may pursue a grievance through VA's administrative or negotiated grievance procedures.

If you believe that you have been the victim of unlawful discrimination on the basis of age, you must either contact an EEO Counselor as noted above or give notice of intent to sue to the Equal Employment Opportunity Commission (EEOC) within 180 days of the alleged discriminatory action.

WHISTLEBLOWER PROTECTION LAWS

A VA manager or supervisor with authority to take, direct others to take, recommend or approve any personnel action must not misuse that authority to take, or fail to take, or threaten to take, or fail to take, a personnel action against an employee or applicant because of disclosure of information by that individual that is reasonably believed to be evidence of violations of law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. The only exception is disclosure of such information specifically prohibited by law and such information specifically required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs.

Retaliation against an employee or applicant for making a protected disclosure is prohibited by 5 U.S.C. 2302(b)(8). If you believe that you have been the victim of whistleblower retaliation, you may report it to the VA OIG (Office of Inspector General) hotline number at 1-800-488-8244, or you may file a written complaint (Form OSC-11) with the U.S. Office of Special Counsel at 1730 M Street NW, Suite 218, Washington, DC 20036-4505, or online through the OSC website, www.osc.gov.

RETALIATION FOR ENGAGING IN PROTECTED ACTIVITY

VA cannot retaliate against an employee or applicant because that individual exercises his or her rights under any of the federal anti-discrimination or whistleblower protection laws listed above.

If you believe you are the victim of retaliation for engaging in protected activity, you must follow, as appropriate, the procedures described in the anti-discrimination and whistleblower protection laws or, if applicable, the administrative or negotiated grievance procedures in order to pursue a legal remedy.

DISCIPLINARY ACTIONS

Under existing laws, VA retains the right, where appropriate, to discipline a manager or supervisor who has engaged in discriminatory or retaliatory conduct, up to and including removal. If OSC has initiated an investigation under 5

U.S.C., however, agencies must seek approval from Special Counsel to discipline employees for, among other activities, engaging in prohibited retaliation.

Nothing in the No FEAR Act alters existing laws or permits VA to take unfounded disciplinary action against a federal employee or to violate the procedural rights of a federal employee who has been accused of discrimination.

ADDITIONAL INFORMATION

For further information regarding the No FEAR Act regulations, refer to links on this site, 5 CFR 724, as well as the appropriate offices within your agency, such as the EEO Manager, Human Resources Management Service or the Office of Resolution Management.

Additional information regarding whistleblower protection can be found at the following websites:

- EEOC Web site – www.eeoc.gov
- OSC Web site – www.osc.gov

EXISTING RIGHTS UNCHANGED

Pursuant to section 205 of the No FEAR Act, neither the act nor this notice creates, expands or reduces any rights otherwise available to any employee, former employee or applicant for employment under the laws of the United States.

ADR MEDIATION PROGRAM

WHAT IS ADR AND THE ADR MEDIATION PROGRAM?

ADR is Alternative Dispute Resolution. ADR provides an arena where employees thoroughly examine all matters related to workplace disputes. The ADR program is available to all employees at NYHHS.

The ADR program was created to actively support local mediation as an alternative forum for the resolution of work-related disputes. Using mediation to resolve differences demonstrates a commitment to a positive approach and joint ownership of concerns and solutions and it can be used any time all parties to a dispute are willing to use it.

Mediation is a process that helps you to find satisfying solutions to your problems. In mediation a neutral person who is not associated with either side facilitates communication between the parties. By exploring ways to resolve the differences, you may be able to reach an agreement that best addresses the parties' interest.

WHAT IS MEDIATION?

- Mediation is used as a problem-solving process.
- Mediation is an informal way parties can resolve workplace disputes.
- Mediation promotes principles and practices that will facilitate communication and working relationships.
- Mediation is a totally voluntary process and can only be pursued if all parties want to participate in the process.
- Mediation involves the parties themselves deciding what is important and who make decisions based on those factors.
- Mediation, unlike arbitration or court proceedings, does not focus on who is right or wrong. It allows the parties to create their own solutions and examine unique solutions to a problem instead of taking the problem to a judge, arbitrator or other outside decision-maker.
- Mediation is a process where a neutral third person, a mediator, acts to encourage and facilitate the resolution of a dispute between two or more parties.

WHAT IS THE ROLE OF THE MEDIATOR?

- The mediator will not decide who is right or wrong. However, the mediator will assist employees in talking about the problem and will help everyone decide how to resolve the problem.
- The mediator assists the parties to identify issues, fostering joint problem-solving and exploring settlement opportunities.
- The mediator has no power to make decisions for the parties or to tell the parties what they should or should not do.
- The mediator helps the parties become the decision-makers by understanding and listening and working together to create options and solutions that meet their concerns. The mediator helps parties communicate with each other to explore ways to resolve their differences and reach an agreement that is realistic and mutually satisfactory.

WHEN CAN I USE MEDIATION?

- When an employee files an EEO complaint with the Office of Resolution Management (ORM), the employee will be offered the ADR mediation process. The ADR mediation program can be used to resolve a variety of differences, including grievances, discrimination complaints, employee-employee disputes, supervisor-employee disputes, patient complaints, service-service disputes and other workplace differences.
- When traditional legal remedies will not solve the problem.
- When parties need to solve a problem and maintain a relationship.
- When privacy is important to one or both parties.

HOW DO I BEGIN THE ADR PROCESS?

The mediation process is initiated by contacting the Mediation Program Coordinator who can discuss your options with you and provide additional information on the process. An agreement must be signed by both parties in order to participate in the ADR mediation process. The Mediation Program Coordinator will also work with you and the other party or parties to make sure both sides agree that mediation is the way to go.

HOW DOES MEDIATION WORK?

The six steps that are necessary components of mediation efforts are as follows:

- Establish ground rules that define how the parties and process will operate during mediation.
- Identify the issues so there is mutual understanding about what the problem is and why it is a problem.
- Identify the interests, concerns and/or limitations of all parties to the dispute. If there is more than one issue in the dispute, the parties should decide the order in which to address them.
- Generate possible solutions to the problem(s).
- Evaluate the potential solutions to identify alternatives that are practical, mutually acceptable and in line with the parties' interests, concerns and limitations.
- Prepare a written agreement to resolve the issues in the dispute.

ARE MEDIATION SESSIONS CONFIDENTIAL?

Yes! The mediation sessions and all materials disclosed during mediation are confidential. Both parties must agree to confidentiality of the parties and the mediation process.

Mediators will not testify or produce records, notes or work products in any future proceedings and no recordings or records will be made of the meeting.

BENEFITS OF MEDIATION

- Mediation is an opportunity to develop unique solutions that are acceptable to both parties.
- Mediation is a confidential process. The mediator must keep all information confidential.
- Mediation is fast. Prompt resolution of a dispute frees participants to resume other activities more quickly.
- Participants retain their rights to pursue other alternatives.

ADR RESOLUTIONS

Resolutions are designed by the individuals involved in the disagreement rather than by an outside person.

An agreed-upon resolution between the parties is the primary goal. Mediation is often considered successful if a better understanding or a better relationship between the participants is achieved.

FOR MORE INFORMATION

Contact Denise Hinton, Mediation Program Coordinator, ext. 3505 (BK) or ext. 3352 (NY).

LIMITED ENGLISH PROFICIENCY (LEP)

This training is designed to familiarize you with accommodating persons with Limited English Proficiency. These are usually referred to as simply “LEP” programs. Limited English Proficiency is defined as the inability to speak, read, write or understand English at a level that permits effective interaction with healthcare providers.

WHO IS A LIMITED ENGLISH PROFICIENT PERSON?

Persons who do not speak English as their primary language and who have a limited ability to read, speak, write or understand English can be limited English proficient, or “LEP.” These individuals may be entitled to language assistance with respect to a particular type of service, benefit or encounter.

OUR LEGAL RESPONSIBILITY

Title VI of the 1964 Civil Rights Act

“No person in the United States shall, on the ground of race, color or national origin, be excluded from participation in, be denied the benefits of or be subjected to discrimination under any program or activity receiving federal financial assistance” (42 U.S.C. §2000d).

Executive Order 13166

To clarify existing requirements for LEP persons under Title VI, on August 11, 2000, President Clinton issued Executive Order 13166, “Improving Access to Services for Persons with Limited English Proficiency.” This requires each federal agency to examine the services it provides and develop and implement a system by which LEP persons can meaningfully access those services consistent with, and without unduly burdening, the fundamental mission of the agency.

Each federal agency is also directed to work to ensure that recipients of federal financial assistance provide meaningful access to their LEP applicants and beneficiaries. To this end, each agency must prepare a plan to improve access to its federally conducted programs and activities (i.e., the services it provides directly to the public) by eligible LEP persons. The approximately 30 federal agencies, including DOT, that provide federal financial assistance to other parties, such as states, must also develop guidance for their recipients on complying with LEP requirements.

OUR AGENCY’S POLICIES ON LEP

VHA Directive 2002-006 (January 31, 2002), Limited English Proficiency (LEP)

This directive issues policy prohibiting discrimination on the basis of national origin for persons with limited English proficiency in federally conducted programs and activities. Equal opportunity laws and VA regulations prohibit discrimination based on national origin. This applies to all programs or activities conducted by VHA and to all programs receiving financial assistance from the Agency.

Healthcare System Policy No. 005-9, Limited English Proficiency (LEP)

This document implements a Limited English Proficiency (LEP) policy at the NYHHS that prohibits discrimination on the basis of national origin for persons with limited English proficiency. It states that no one can be subjected to any form of discrimination because of national origin in any VHA program or in programs receiving VA funding or in any VA program’s federal financial assistance.

A listing will be updated annually of staff proficient in languages other than English and volunteer translation services available during normal shift assignments. NYHHS utilizes a translator telephone by CYRACOM International available in patient care areas. The EEO Specialist also has contacts with outside interpreters.

The policy also states that the healthcare system will ensure timely processing of all external civil rights and equal opportunity discrimination complaints, and that the EEO/Affirmative Employment Specialist is performing this function timely and accurately.

FOUR MAJOR LANGUAGE GROUPS

Most individuals living in the United States read, write, speak and understand English. There are many individuals, however, for whom English is not their primary language. For instance, based on the 2000 census, over 26 million individuals speak Spanish and almost 7 million individuals speak an Asian or Pacific Island language at home. If these individuals have a limited ability to read, write, speak or understand English, they are Limited English Proficient

(LEP). Language for LEP individuals can be a barrier to accessing important benefits or services, understanding and exercising important rights, complying with applicable responsibilities or understanding other information provided by federally funded programs and activities.

Spanish includes those who speak Ladino. **Other Indo-European languages** include most languages of Europe and the Indic languages of India. These include the Germanic languages, such as German, Yiddish and Dutch; the Scandinavian languages, such as Swedish and Norwegian; the Romance languages, such as French, Italian and Portuguese; the Slavic languages, such as Russian, Polish and Serbo-Croatian; the Indic languages, such as Hindi, Gujarathi, Punjabi and Urdu; Celtic languages; Greek; Baltic languages; and Iranian languages.

Asian and Pacific Island languages include Chinese; Korean; Japanese; Vietnamese; Hmong; Khmer; Lao; Thai; Tagalog or Pilipino; the Dravidian languages of India, such as Telegu, Tamil and Malayalam; and other languages of Asia and the Pacific, including the Philippine, Polynesian and Micronesian languages.

All other languages include Uralic languages such as Hungarian; the Semitic languages such as Arabic and Hebrew; languages of Africa; native North American languages including the American Indian and Alaska native languages; some indigenous languages of Central and South America.

DO'S AND DON'TS

- DO treat every client as a client regardless of his or her ability to speak English.
- DON'T get caught up in trying to assess whether or not a person can speak English if he/she wanted to. We are not in the foreign language assessment field.
- DON'T suggest, expect or even allow minors to act as interpreters.
- DON'T suggest, expect or even allow other clients to act as interpreters. Even for scheduling appointments, the fact that someone is a client is protected healthcare information under HIPAA and cannot be discussed without the client's permission--which you can't get unless you communicated with him or her first.
- DO clearly document any instance when you believe the circumstances warranted the use of an interpreter whose qualifications you are not familiar with.
- DO clearly document, every time, any occasion when a friend of the client or a family member is used as an interpreter. Did the client make the decision, after being clearly informed that they have a right to free language assistance?

PATIENT SAFETY PROGRAM & PERFORMANCE IMPROVEMENT

PATIENT SAFETY PROGRAM

It is the policy of our patient safety program to:

- Foster patient safety.
- Aggregate data.
- Formulate corrective actions.
- Communicate safety issues.
- Encourage reporting of actual and potential (close call) adverse events.

The following methods are used to foster patient safety:

- Report events using VA Form 10-2633.
- Participate on Root Cause Analysis (RCA) Teams.
- Healthcare Failure Mode and Effect Analysis (HFMEA).

The following agencies promote patient safety:

- VA National Center for Patient Safety (NCPS)
- Joint Commission (JCAHO)
- NASA Patient Safety Reporting (PSRS)

Examples of adverse patient events include but are not limited to:

- Medication errors
- Adverse drug events
- Transfusion errors
- Patient falls
- Missing patients
- Suicides
- Medical device events
- Equipment related events
- Patient misidentifications
- Delays in treatment
- Suicide attempts
- Suicide gestures

For more information on the patient safety program, see NYHHS Policy No. 00-14.

Importance of Reporting Actual or Close Call Events

NYHHS promotes an organizational “blame-free” culture of safety. Report close calls and actual events to:

- Prevent recurrence
- Ensure patient and staff safety
- Prevent adverse or sentinel events
- Improve hospital processes and communication

Patient Safety Statistics

- 44,000-98,000 deaths occur each year as a result of medical errors.
- The healthcare industry spends \$17-29 billion on preventable adverse events which cause injury.

Staff are encouraged to:

- Report all adverse events and close calls
- Report all incidents resulting in harm or with potential to harm patients
- Remember: Anyone can make a mistake. However, the mistake cannot be corrected unless it is identified, acknowledged, reported and analyzed and the issues that lead or contributed to the mistake are resolved.

Procedure for Identification and Reporting of Adverse Events

- Regardless of position or discipline, the employee who witnesses, or who is the first to become aware of the incident, will initiate the incident report. (This form is not to be used for incidents which involve visitors or employees.)

- If the employee who first becomes aware of the incident is a non-clinical staff member, he/she will ask the clinical staff to assist in the completion of the incident report.

Staff's Role in Patient Safety Reporting and Improvement Initiatives

- Report immediately all actual or potential adverse events.
- Protect the patient from further harm.
- Submit the necessary/appropriate documents.
- Actively participate in performance improvement activities such as:
 - Data collection and monitoring activities
 - Root Cause Analysis (RCA)
 - Identifying processes for improvement
 - Supporting fellow employees' performance improvement initiatives

JCAHO 2006 National Patient Safety Goals

Goal 1: Improve the accuracy of patient identification.

Goal 2: Improve the effectiveness of communication among caregivers.

Goal 3: Improve the safety of using medications.

Goal 4: Eliminate wrong site, wrong patient, and wrong procedure/surgery.

Goal 5: Improve the safety of using infusion pumps.

Goal 6: Improve the effectiveness of clinical alarm systems.

Goal 7: Reduce the risk of healthcare-associated infections.

Goal 8: Accurately and completely reconcile medications across the continuum of care.

Goal 9: Reduce the risk of patient harm resulting from falls.

Goal 10: Reduce the risk of influenza and pneumococcal disease in institutionalized older adults.

Goal 11: Reduce the risk of surgical fires.

Goal 12 (Not Applicable): Implement applicable National Patient Safety Goals and associated requirements by components and practitioner sites.

Goal 13 (New): Encourage the active involvement of patients and their families in the patient's own care as a patient safety strategy.

Goal 14 (New): Prevent healthcare-associated pressure ulcers (decubitus ulcers).

Highlights of Patient Safety Goal 1: Identifying the Patient

- Use Active NOT passive techniques: When giving medications, blood products, taking specimens, performing procedures or providing care, ask the patient to state his/her name. Do NOT state the patient's name.
- Use at least two patient identifiers to confirm ID:
 - Name
 - Date of birth
 - Social security number
 - Picture
 - Telephone number

Highlights of Patient Safety Goal 2: Improve Communication - Clarify the Message

- Write down and then read back what you heard when taking verbal and telephone orders and critical laboratory, radiology or other diagnostic test results.
- Spell it out if in doubt.
- Limit abbreviation use.
- Avoid UN-wanted abbreviations found in Chief of Staff Memorandum No. 03-02A.

Highlights of Patient Safety Goal 4: Use Correct Site Techniques

- Step 1: Consent form - Include the reason for the procedure and location of its site.
- Step 2: Mark the site of the procedure/operation - done by the physician team member; include the patient whenever possible.
- Step 3: Patient ID - Use active technique: Patient states their name AND SSN or date of birth and the procedure site.
- Step 4: "Time Out" with the patient present in the OR/Procedure Suite/at bedside for procedure; staff verbally confirms patient, site, position and implant (if applicable).
- Step 5: Imaging data – Two or more members confirm the image label and orientation.

Highlights of Patient Safety Goal 7: Reduce the Risk of Health Care-Associated Infections

- Comply with VA Directive 2005-002, Required Hand Hygiene Practices.
- Use an alcohol-based hand rub or antimicrobial soap and water to routinely decontaminate hands before and after direct contact with a patient.

Highlights of Patient Safety Goal 8: Accurately and Completely Reconcile Medications Across the Continuum of Care

- Make a list and document all medications that the patient takes outside at home whenever he/she begins care at NYHHS.
- Include any herbal and over-the-counter medications.
- Update the list every time the patient receives care in a different part of NYHHS.

Highlights of Patient Safety Goal 9: Reduce the Risk of Patient Harm Resulting from Falls

- Assess and re-assess each patient's risk for falling.
- Include the potential risks that may be associated with the patient's medication regimen.
- Take action to address any identified risk(s).
- Implement a fall prevention program.

Remember: Improving patient safety is everyone's responsibility.

PERFORMANCE IMPROVEMENT

At NYHHS all staff are committed to quality patient care and improving outcomes. A Plan for Performance Improvement outlines the specific performance improvement goals and shows how these are linked to the Mission, Vision and Values. NYHHS uses a collaborative, interdisciplinary improvement approach that utilizes the Plan, Do, Check, Act (PDCA), Cycle, also known as the Shewhart Cycle. This cycle provides a systematic approach to performance improvement involving four steps:

Step 1 - **Plan:** Organizing a team to study the process and to decide what change might improve it. Data collection and analyzes are required.

Step 2 - **Do:** Carry out the change or test on a small-scale basis.

Step 3 - **Check:** Observe the effect of the change or test.

Step 4 - **Act:** Study the results. What was learned? Repeat the test if necessary. If the change results in the desired outcome, standardize the change and maintain the improvement. If the desired outcome was not achieved, return to step 1 and repeat the process.

For more information contact:

Dea Hughes, NYHHS Patient Safety Manager, NY ext. 2113; BK ext. 3879

Kim Arslanian, NYHHS Performance Improvement Manager, BK ext. 2865

Alan Wikler, NYHHS Deputy Performance Improvement Manager, NY ext. 4545

Stephanie Berkson, NYHHS Accreditation Specialist, NY ext. 6812

Telma Hall, RN, QM/UM Coordinator, NY ext. 3476

Antoinette Ianelli, RN, QM/UM Coordinator, BK ext. 3676

Sally Bright-Philpot, RN, QM/UM Coordinator, SA ext. 2412

RESIDENT SUPERVISION: SUPERVISING PRACTITIONER RESPONSIBILITIES

All VA care is provided either by a licensed independent practitioner with appropriate privileges (e.g., an attending physician) or by a resident physician under the direction of an attending physician, who is called the supervising practitioner (SP). All patient encounters or reports of patient diagnostic examinations must identify the supervising practitioner (SP) and indicate the level of involvement.

There are four ways to document resident supervision:

- The SP writes his/her own progress note.
- The SP writes an addendum to the resident's note.
- The SP countersigns the resident's note (which implies that the SP concurs with the resident's note). Reports related to reviews of patient material (e.g., pathology, radiology) must be verified and countersigned by the SP.
- The resident documents the SP's supervision in his/her note. The SP's name, level of involvement and concurrence with the plan are essential elements (e.g., "I have seen and discussed the patient with my supervising practitioner, Dr. X and Dr. X agrees with the assessment and plan").

INPATIENT SERVICE

NEW ADMISSION – The SP must evaluate the patient within 24 hours of admission.

Documentation – The SP writes a note or adds an addendum to the resident's note documenting the SP's findings and therapeutic plan. The documentation must be by the end of the calendar day following admission.

CONTINUING CARE – The attending must be personally involved in the patient's ongoing care.

Documentation – Any of the four methods listed above is sufficient, at a frequency consistent with the patient's clinical acuity and principles of graduated levels of responsibility. It is NYHHS's goal that every resident note be so documented.

DISCHARGE OR TRANSFER – The attending must be personally involved in a decision to discharge or transfer the patient to another service or to another level of care.

Documentation – The SP must countersign the discharge/transfer note. If the patient is transferred to another inpatient service, the accepting service's SP must treat the patient as a new admission.

OUTPATIENT SERVICE

The SP must be physically present in the clinic.

NEW VISIT – Every new patient must be seen by or discussed with the SP.

Documentation – Any of the four types of documentation listed above is sufficient.

RETURN VISIT – Patients must be seen by or discussed with the SP at a frequency to ensure appropriate treatment.

Documentation – Any of the four types of documentation listed above is sufficient.

DISCHARGE – The SP will ensure the patient's discharge from the clinic is appropriate.

Documentation – Any of the four types of documentation listed above is sufficient.

CONSULTATIONS (INPATIENT, OUTPATIENT, EMERGENCY DEPARTMENT)

The SP must supervise all consults performed by the residents.

Documentation – Any of the four types of documentation listed above is sufficient.

RADIOLOGY AND PATHOLOGY

Documentation – Reports related to reviews of patient material must be verified and countersigned by the radiology or the pathology SP.

EMERGENCY DEPARTMENT

The Emergency Department SP must be physically present in the Emergency Department and is the attending of record for all Emergency Department patients. The Emergency Department SP must be involved in the disposition of all Emergency Department patients.

Documentation – Any of the four types of documentation listed above is sufficient.

SURGERY

Except in emergencies, the SP must evaluate each patient pre-operatively.

Documentation – The SP must write a pre-procedure note detailing findings, diagnosis, therapeutic plan and choice of surgical procedure (may be done up to 30 days prior to surgery). Informed Consent must be obtained according to NYHHS policy. The attending's level of involvement is documented in the VistA Surgical Package. Post-operative documentation is required following JCAHO standards and NYHHS's Bylaws, Rules and Regulations of the Medical Staff (available on the organization's intranet site on the Documents page under the heading NYHHS Clinical Documents).

PROCEDURES

ROUTINE PROCEDURES (e.g., lumbar punctures, central line placements, paracenteses)

Graduated Levels of Responsibility apply. The resident must write a procedure note that includes the SP's name.

Documentation – Any of the four types of documentation listed above is sufficient.

NON-ROUTINE AND NON-OPERATING ROOM PROCEDURES (e.g., cardiac catheterization, endoscopy, interventional radiology)

The SP must authorize the procedure and be physically present in the procedure area.

Documentation – Any of the four types of documentation listed above is sufficient.

OPERATING ROOM PROCEDURES

The attending's level of involvement is documented in the VistA Surgical Package using the following codes:

Level A (Attending Doing the Operation) – The SP performs the case; the resident may assist.

Level B (Attending in the OR and Scrubbed) – The SP is physically present in the OR and is directly involved in the procedure. The resident performs the major portions of the procedure.

Level C (Attending in the OR but Not Scrubbed) – The SP is physically present in the OR providing direction to the resident.

Level D (Attending in the OR Suite, Immediately Available) – The SP is physically present in the OR suite and is immediately available for supervision or consultation as needed.

Level E (Emergency Care) – Immediate care is necessary to preserve the patient's life or prevent serious impairment. The attending must be contacted.

Level F (Routine Bedside or Clinic Procedure Done in the OR) – The attending is identified.

Reference: VHA Handbook 1400.1 Resident Supervision, May 3, 2004.

NOTE: Resident supervision guidelines are subject to occasional revision. All staff and trainees are advised to check with their supervisors for updated requirements.

PAIN MANAGEMENT

NYHHS is committed to prompt recognition and compassionate alleviation of patients' pain.

DEFINITION OF PAIN

- Pain is an unpleasant sensory and emotional experience with actual or potential tissue damage.
- Pain can affect daily functioning, sleep, appetite, mood and relationships.
- Pain is subjective and is what the patient experiencing it says it is.
- Pain Management is integral to patient care and is a patient's right.

PAIN ASSESSMENT

- The patient's self-report is the single most reliable indicator of pain.
- Pain Intensity Rating scales are used by staff to assess a patient's pain level.
- Pain Intensity Rating scales are posted in every patient room.

HOSPITAL EMPLOYEES' ROLE IN PAIN MANAGEMENT

- To communicate the patient's report of pain to his/her treatment team.
- To encourage the patient to report any pain to his/her treatment team.

THE PATIENT'S ROLE IN PAIN MANAGEMENT

- The patient has an active role in the treatment of his/her pain.
- The patient should tell the treatment team if he/she has pain and if the pain therapy is working.

VHA COMPLIANCE & BUSINESS INTEGRITY PROGRAM

The purpose of the Compliance and Business Integrity (CBI) Program is to ensure that VA's business operations follow all laws, regulations and policies that apply and to promote standards of excellence in business practices. VA's CBI Program follows the Office of Inspector General's Compliance Program Guidance for Hospitals using the seven elements of an effective compliance program.

VA STANDARDS OF ETHICAL CONDUCT

The following standards apply to all employees as well as some other individuals who might not be considered traditional employees such as residents, consultants and fee basis individuals. Individuals who have questions about their applicability of the ethical rules should contact their local Compliance Office for more information.

- I. Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain.
- II. Employees shall not hold financial interests that conflict with the conscientious performance of duty.
- III. Employees shall not engage in financial transactions using nonpublic government information or allow the improper use of such information to further any private interest.
- IV. An employee shall not solicit or accept any gift or other item of monetary value, from any person or entity seeking official action from, doing business with, or conducting activities regulated by the employees agency, or whose interests may be substantially affected by the performance or non-performance of the employee's duties.
- V. Employees shall put forth an honest effort in the performance of their duties.
- VI. Employees shall not knowingly make unauthorized commitments or promises of any kind purporting to bind the government.
- VII. Employees shall not use public office for private gain.
- VIII. Employees shall act impartially and not give preferential treatment to any private organization or individual.
- IX. Employees shall protect and conserve federal property and shall not use it for other than authorized purposes.
- X. Employees shall not engage in outside employment or activities, including seeking or negotiating for employment, that conflict with official government duties and responsibilities.
- XI. Employees shall disclose waste, fraud, abuse and corruption to appropriate authorities.
- XII. Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those such as federal, state or local taxes that are imposed by law.
- XIII. Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age or handicap.
- XIV. Employees shall endeavor to avoid creating the appearance that they are violating the law or the ethical standards set forth in this part. Whether particular circumstances create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the relevant facts.

COMPLIANCE TERMS

Fraud and Abuse

Fraud is the act of intentionally submitting false information (or omitting true information) in order to obtain payment from an insurance company or Medicare. Abuse occurs when a provider unintentionally submits false information, but should have known better had the provider been familiar with the Medicare manual or updates from the Fiscal Intermediary.

Self-Referrals

Self-referrals are those that in any way financially benefit the referring provider. VA contracting physicians are prohibited from referring patient to themselves, family members or to organizations from which they can benefit.

False Claims Act

Parties who knowingly present fraudulent claims for payment to the government can be fined as much as \$10,000 per violation.

DOCUMENTATION AND CODING (FOR CLINICIANS)

Clinicians are responsible for complete and accurate documentation of the care provided to the patient. This information is necessary for research, epidemiology, reimbursement, evaluation of quality of care and communication to support the patient's treatment. The Computerized Patient Record System (CPRS) is utilized to document all patient care and services. The electronic encounter form within CPRS will be utilized in outpatient services to capture diagnostic and procedure codes.

TEACHING PHYSICIAN RULES FOR VA

VA bills in the name of the attending physician rather than the resident when billing for care in a properly supervised environment. A "GC" modifier is applied to each CPT code in order to distinguish care provided by a resident under the direction of a teaching physician. VHA Handbook 1400.1, "Resident Supervision" is the primary guidance for the documentation of care in teaching settings.

YOUR ROLE IN THE ORGANIZATION

Any agent of the facility who is aware of potential violations of law or business practices are obligated to report the activity to the supervisor of their service or to the facility's Chief Compliance Officer (Kathleen Gaine, ext. 3566 at the Brooklyn Campus or at the NY Campus Compliance Office, ext. 5944 or ext. 3589). Issues will be reviewed and corrective action taken. If you want to report potential violations anonymously, a CBI HelpLine has been established. The CBI HelpLine number is 1-866-842-4357. The HelpLine is available 24 hours a day and the caller may remain anonymous.

VHA PRIVACY POLICY TRAINING

APPLICABLE CONFIDENTIALITY STATUTES AND REGULATIONS

The following legal provisions govern the collection, use, maintenance and disclosure of information from VHA records:

- The Freedom of Information Act (FOIA) (5 U.S.C. 552)
- The Privacy Act (5 U.S.C.552a)
- 38 U.S.C 5701 - The VA Claims Confidentiality Statute
- 38 U.S.C 7332 - Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records
- 38 U.S.C. 5705 - Confidentiality of Healthcare Quality Assurance Review Records
- The HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164

Freedom of Information Act (FOIA)

- FOIA compels disclosure of reasonably described VHA records or a reasonably segregated portion of the records to any person upon written request, unless one or more of the nine exemptions from the general disclosure requirement apply. Generally, VHA is not required to release individually identifiable veteran information under FOIA.
- Contact the FOIA Officer if you receive, or have questions regarding, a FOIA request.

Privacy Act of 1974

- Provides for the confidentiality of information about an individual that is retrieved by the individual's name or other unique identifier, such as the SSN.
- Such information is contained in a system of records and must be protected.
- Prohibits disclosure of any record contained in a system of records unless specifically authorized by the Act.
- Provides rights to the individual by whose name VHA retrieves the information.
- Contact your facility Privacy Officer with questions regarding the Privacy Act and systems of records.

38 U.S.C. 5701 (VA Claims Confidentiality Statute)

- Provides for the confidentiality of all VHA patient claimant information, with special protection for their names and home addresses.
- Provides for the same for information about their dependents.
- Prohibits disclosure of these names and addresses except as authorized by the statute.
- Does not apply to employee information.

38 U.S.C. 7332

- Provides for the confidentiality of VHA-created individually identifiable Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records and Health Information.
- Prohibits use or disclosure with a few exceptions. VHA may use the information to treat the patient who is the record subject.
- Must have specific written authorization in order to disclose in most cases, including for treatment by a non-VA provider.

38 U.S.C. 5705

- Provides for the confidentiality of Healthcare Quality Assurance (QA) Review Records.
- Records created by VHA as part of a designated medical quality assurance program are confidential and privileged.
- VHA may disclose this data in only a few, limited situations.
- Contact your facility Privacy Officer if you collect QA data, or have questions concerning the use or disclosure of Section 5705 protected information.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Privacy Rule provides confidentiality for VHA patients' protected health information (PHI). The Privacy Rule:

- Authorizes VHA to use or disclose information without a patient's prior written authorization for VHA treatment, payment or healthcare operations.
- Prohibits other uses and disclosures of PHI except as authorized by the regulation or with a prior written authorization.

- Provides rights to the individuals to whom the PHI pertains.

Payment

- A payment is an activity undertaken by VHA to determine its responsibility for coverage or to provide reimbursement for health care.
- This could include pre-certification, utilization review or release of protected health information (PHI) to a third-party insurance carrier for VHA reimbursement for care provided.

Treatment

- Treatment is defined as the coordination or management of health care or related services by one or more healthcare providers. VHA is a healthcare provider.
- This includes the coordination of health care by a healthcare provider with a third party, consultation between providers relating to a patient and the referral of a patient for health care from one healthcare provider to another.

Healthcare Operations

- Healthcare operations are those activities which are deemed essential to the effective operation of a VHA medical facility.
- These include conducting quality assessment and improvement activities, case management, reviewing competence or qualification of healthcare professionals, evaluating practitioner performance, legal services, business management, auditing and customer service evaluations.

Relationship Between Laws

- VHA employees must comply with all applicable privacy laws and regulations when:
 - Accessing, using or disclosing information
 - Processing requests from individuals exercising their privacy rights
- When conflicts arise:
 - The more stringent law or regulation applies for uses and disclosures
 - The one that affords the greatest rights to the individual applies for privacy rights
- Refer to VHA Handbook 1605.1, Privacy and Release of Information, and/or contact the Privacy Officer if you have questions.

COMPLIANCE WITH PRIVACY POLICIES

- All employees must conduct themselves in accordance with the rules of conduct concerning the disclosure or use of information.
- All employees and some contractors must sign the Statement of Commitment and Understanding.
- VHA privacy policy is contained in VHA Directive 1605 and VHA Handbook 1605.1, Privacy and Release of Information.
- Failure to comply with privacy policies could lead to significant civil penalties for the agency and disciplinary or other adverse action or criminal penalties for the employee.

Use of Information

- Remember, VHA employees must comply with all six statutes and regulations, where applicable, when using, accessing or disclosing information.
- VHA employees may access information in order to perform their official duties related to the treatment of veterans, the payment for care provided by VHA and/or the healthcare operations of VHA.

Incidental Disclosures

- Privacy policy allows for the following incidental uses and disclosures of individually identifiable health information:
 - Posting patient names outside rooms
 - Pharmacy Bingo boards (with limited information)
 - Patient sign-in sheets (no SSN or diagnoses)
 - Calling only the patient's name in a waiting area
 - Ward "white boards" (with limited information)
 - Curtains dividing treatment areas in emergency areas instead of separate rooms
- Contact the Privacy Officer with questions about whether other conduct may be an incidental disclosure.

Disclosure of Information

- VHA generally is not obligated to release information.
- The general rule is that the use or disclosure of protected health information is prohibited unless authorized by all applicable confidentiality statutes and rules. Commonly permitted disclosures include:
 - For treatment, payment or healthcare operations

- Authorized by the patient, or
- Required for public health and/or certain law enforcement purposes, or
- Where required by law, including pursuant to a qualifying court order

What Can Be Disclosed?

- Under some circumstances, it is necessary for non-ROI (Release of Information) staff to release information. Written requests must be obtained from the requestor so that these can be accounted for in the ROI software.
- Clinicians may provide information directly to a patient for purposes of patient education without obtaining a written request.

Authorization Requirement

- Any authorization for release of medical information must be in writing and contain all required elements. Verbal authorizations are unacceptable under applicable federal law.
- Most requests for records should be processed by the Release of Information (ROI) Unit.
- VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, meets the authorization requirements.
- VA Form 10-5345a, Individual's Request for a Copy of Their Health Information, meets the written request requirement when veterans request copies of their own health information.

Exception to Need for Authorizations

- There are situations where a disclosure may be made without an authorization, for example, public health reporting:
 - Disclosure to public health authorities charged with protection of the public may be done only with a standing written request or other applicable legal authority.
- Contact the Privacy Officer for additional information on situations where an authorization is not required.

Research

- VA research requests must have approval from the Research & Development Committee and an Institutional Review Board (IRB).
- Because the privacy requirements to use health information for research are complex, the Privacy Officer or Research Compliance Officer should be contacted for assistance.
- For further information review VHA Handbook 1605.1, Privacy and Release of Information, paragraph 13.

Minimum Necessary Standard

- Requests for, and disclosures of, information must be limited to only the minimum amount necessary to accomplish the needed purpose.
- Healthcare providers must be given what is needed for continuity of care and for treatment purposes.
- Employees must have the minimum necessary amount of information to do their official job.
- Contact the Privacy Officer for more information.

Functional Category

- Each employee must have a functional category assigned to them.
- Functional categories identify the appropriate level of access to protected health information.
- See VHA Handbook 1605.2, Minimum Necessary Standard for Protecting Health Information.

Facility Directory Opt-Out

- Except in limited circumstances, a VHA facility will ask a patient upon admission whether s/he wishes to be in the Patient Facility Directory.
- If the patient does not object, the facility may tell anyone who asks for the patient by name the patient's name, location and general medical condition.
- If the patient objects to inclusion in the Directory, the facility identifies the patient by "!" on the Gains and Losses Report and in VistA Patient Inquiry, and cannot release any information whatsoever to anyone who asks for the patient. The facility contact should say, "I am sorry but I have no information that I can give you on whether Mr. X is a patient."
- Patients may change their mind about being in the Directory at any time during their admission.

VETERANS' PRIVACY RIGHTS

VA patients have several privacy rights in their VHA patient records, including the right to:

- Receive a notice of VHA's privacy practices
- Request access to his/her VHA medical records

- Request restrictions on VHA's use and disclosure of the records
- Request that VHA amend the medical records
- Request an accounting of VHA's disclosures of the records
- Ask VHA to communicate with the patient about his medical care in certain agreed methods
- File a complaint about any VHA conduct with the patient's PHI that the patient believes violates the HIPAA Privacy and Security Rules

Veterans' Notice and Access Rights

- Notice of privacy practices: VA must periodically notify veterans in writing how VA may use or disclose their protected health information, how they may exercise their privacy rights and how they may submit privacy complaints.
- Access: Veterans have the RIGHT to request and receive copies of their records. Facilities should infrequently deny access requests. Access requests must be processed as stated in VHA Handbook 1605.1, paragraph 7. The veteran must be notified of any denial of access in writing and provided appeal rights.

Veterans' Right to Request Restrictions

- Veterans have the right to request restrictions on the use and disclosure of their information.
- The request must be in writing and signed by the veteran; however, VHA is not required to grant restriction requests. You are to follow the procedure in VHA Handbook 1605.1, paragraph 11, in processing requests for restrictions. In most cases, such requests will be denied.

Veterans' Right to Amendment

- The veteran has the right to request an amendment to any information in his/her record.
- The request must be in writing and adequately describe the specific information the veteran believes to be inaccurate, incomplete, irrelevant or untimely, as well as the reason for this belief.
- All requests for amendment will be reviewed by the facility Privacy Officer and the author of the information being disputed by the veteran.
- The veteran must be notified of any denial of amendment in writing and provided appeal rights, the opportunity to file a statement of disagreement, and the opportunity to have his original request letter and the facility denial letter attached to the disputed information if a statement of disagreement is not filed.

Veterans' Right to Accounting of Disclosure

- VHA medical facilities are required to keep, and a veteran may request, a list of all disclosures of information, both written and oral, from records pertaining to the individual, subject to certain legal exceptions.
- Accountings are not required when the information is requested for performance of official VHA employee duties.
- VHA Handbook 1605.1, paragraph 9, has more information on accounting.

Veterans' Right to Confidential Communication

- An individual has the right to request and receive communications confidentially by an alternative means (for example, in person) or at an alternative location (address other than the individual's permanent address)
- Current VHA policy is not to honor a request to receive communications via e-mail because currently e-mail exchanges with patients are not sufficiently secure to protect the information.

Veterans' Right to File a Complaint

- Patients may file a written complaint about VHA's handling of the patients' information with the Privacy Officer, the Office of Inspector General, the VHA Privacy Office or with the Department of Health and Human Services, Office for Civil Rights.
- The facility must respond in writing to the complainant and put the information into the Privacy Violation Tracking System (PVTS).

HHS Privacy Complaints

- If a VHA facility receives a complaint directly from the Department of Health and Human Services (HHS) Office for Civil Rights, contact the facility Privacy Officer immediately.
- The Privacy Officer will contact the VHA Privacy Office and VHACO (VHA Central Office).
- Contact the VHA Privacy Office to coordinate all responses to a complaint.

TRAINING

- A new VHA employee must receive VHA privacy training within 30 days of entrance on duty.
- All VA employees must complete privacy training annually.
- "Employees" include FTTE, consultants and attendings, without compensation, fee basis, contractors, students and volunteers.
- CWT (Compensated Work Therapy) workers are not considered employees and cannot access individually identifiable patient information without the facility first obtaining proper written authorization from the patient.

PENALTIES

- Civil penalties: \$100 per violation, up to \$25,000 per person per year for all violations of a requirement.
- Criminal penalties for knowing violations include:
 - Up to \$50,000 and one year in federal prison.
 - Under "false pretenses" - up to \$100,000 and up to five years in federal prison.
 - "Intent to sell, transfer or use" - up to \$250,000 and up to 10 years in federal prison.
- In addition to the penalties listed above, administrative, disciplinary or other adverse actions (e.g., admonishment, reprimand or termination) may be taken against employees who violate any of the applicable legal provisions.

OPERATIONAL PRIVACY ISSUES

- Faxes: Information may only be faxed when:
 - No other means exists to provide the requested information in a reasonable manner or time frame.
 - The fax machine is in a secure location.
 - Reasonable steps have been taken to ensure that the fax transmission is sent to the appropriate destination.
- Email: No protected health information (PHI) should be sent unencrypted via Outlook. PHI should be encrypted prior to transmission using VHA-approved means.

REASONABLE SAFEGUARDS

- Computer security:
 - Log off or lock workstation.
 - Turn computer screen/monitor so that it is not visible by people passing by,
 - Secure passwords.
- Office security:
 - Protect information that is on your desk.
 - Lock doors to rooms containing medical records.
 - Lock file cabinets containing health information or other individually identifiable information (employee or veteran).
- Document shredding: NO protected health information should be discarded in regular wastebaskets. All confidential information should be shredded to ensure patient privacy.
- Open Discussions: Absolutely NO health information should be the topic of discussion outside the clinical setting. This includes in places such as the hallway, the canteen, elevators or the parking lot.

Protecting the privacy of veterans' information is an important part of providing quality health care AND is everyone's responsibility. Any privacy questions or concerns should be directed to the Privacy Officer.

HEALTHCARE ETHICS

ETHICS ADVISORY COMMITTEE

The **Ethics Advisory Committee (EAC)** helps to promote ethical healthcare practices through:

- Education - promoting staff understanding of ethics issues
- Consultation – facilitating ethical clinical and administrative decision-making by resolving ethical conflicts, disagreements or uncertainties
- Policy – shaping ethical healthcare policies

When people experience ethical tensions in any of the following areas, they should involve the EAC:

- Shared decision making – e.g., informed consent, advance directives, surrogate decision making
- End of life care – e.g., DNR orders
- Privacy and confidentiality – e.g., accessing/releasing records
- Professionalism – e.g., truth telling, boundaries
- Resource allocation – e.g., relating to access to care

To request an ethics consultation: at the NY campus, page (917) 469-9930 or call the Chief of Staff's Office at ext. 7104; at the BK campus, call the Chief of Staff's office at ext. 3310 or the Patient Representative at ext. 3510. At the SA campus call Social Work at ext. 2351. During WHEN hours (weekend, holiday, evening and night hours) contact the nursing supervisor or the administrator on duty (AOD).

COMMON HEALTHCARE ETHICS PRACTICES

Informed Consent

- Assess the patient's capacity to make the specific decision
- Inform the patient of proposed treatments and alternatives
- Discuss the risks and benefits of each
- Allow the patient to ask questions and raise concerns
- Ensure that the patient understands the information
- Ensure that the patient is making the decision voluntarily
- Document the informed consent process

Advance Directives (AD)

An Advance Directive (AD) is an expression of a patient's wishes regarding treatment preferences to be implemented in the event that the patient loses the capacity to make healthcare decisions. It is usually a written document, but statements made by a patient may also be valid indicators of the patient's preferences. A patient may designate a healthcare proxy to make treatment decisions in the event the patient loses decision-making capacity. An AD may include a Living Will, a treatment preference form, or a durable power of attorney for healthcare (proxy). AD documents must be dated and signed by the patient and two witnesses. An AD can be rescinded by the patient at any time for any reason. AD information for a patient is found in CPRS under "Postings" on the "Cover Sheet" tab.

Do Not Resuscitate (DNR) Orders

The patient or authorized surrogate must expressly agree to have a DNR order written. Regardless of DNR status, all treatments to which the patient consents should continue. The attending physician is responsible for writing the DNR order and entering a progress note in the chart. However, in the physical absence of the attending a resident may write a DNR order, but only after discussion with the attending and documentation of that discussion in the chart and the attending physician must enter a DNR order and progress note within 24 hours. At the NY and BK campuses orders are valid for 7 days; at the SA Extended Care Center orders are valid for 90 days.

Privacy and Confidentiality

Patient records should only be viewed on a need to know basis. Patient information should not be discussed in public spaces such as dining areas, elevators, hallways, buses and shuttles. Patients may view their information online through <http://www.myhealthvet.va.gov/>. Patients must give consent prior to the release of health information. Information about patients with the following diagnoses is specially protected in VA and cannot be released without specific written consent: HIV/AIDS, sickle cell disorder, substance abuse and alcohol abuse.

For further information and specific guidance on ethical healthcare practices, refer to the NYHHS policies on Patient Rights & Responsibilities, the Ethics Advisory Committee, Organizational Ethics, Informed Consent, Advance Directives and Guidelines for Do Not Resuscitate (DNR) Orders.

GIFTS TO HEALTHCARE PROVIDERS FROM THE PHARMACEUTICAL INDUSTRY

This training module is based on excerpts from the report "Gifts to Healthcare Professionals from the Pharmaceutical Industry," by the National Ethics Committee of VHA, October 2003, authored by Paul J. Reitemeier, PhD, Judy Ozuna, ARNP, MN, CNRN, Randy Taylor, PhD, MBA, Jeni Cook, DMin; and Ellen Fox, MD

In an effort to influence practitioners' prescribing practices, the pharmaceutical industry employs diverse marketing and promotional strategies, among them offers of free drug samples, educational materials, meals and other forms of gifts. These efforts are both intensive and expensive. In 2001 the drug industry spent more than \$16 billion on visits to physicians' offices. In the last five years the number of pharmaceutical company sales representatives in the U.S. has increased from 42,000 to 88,000. Some 80% of physicians report having been offered cash or gifts from pharmaceutical industry representatives. Many physicians meet with pharmaceutical industry representatives four or more times per month.

This module addresses gifts provided to individual healthcare professionals by representatives of the pharmaceutical industry. Often these gifts consist of items that are designed to enhance patient care (e.g., reflex hammers, anatomical models) or learning (e.g., meals at educational events, textbooks), but gifts may also be of a more personal nature (e.g., organizers, event tickets). The promotional nature of gifts may be subtle or obvious, depending on, for example, whether a sponsor or product name is prominently displayed. In the following discussion, gifts are distinguished from purely promotional items that have no intrinsic value to the recipient (e.g., product brochures) and from compensation for professional work (e.g., honoraria). Although the analysis offered here was developed specifically in reference to gifts from pharmaceutical representatives, it applies equally to gifts from representatives of medical manufacturers.

WHAT IS A GIFT?

Webster defines a gift as: "something bestowed voluntarily and without compensation." Although this definition captures our casual understanding of a gift as something given with no expectation that the recipient will reciprocate, it misses much of the social aspect of gifts that make gifts from pharmaceutical representatives to healthcare professionals ethically challenging. Unlike contracts, in which parties set out clear, explicit expectations, gifts place people in binding personal relationships that generate vague, open-ended moral obligations. The importance of a gift lies in the personal relationship it generates, sustains and signifies.

WHY ARE GIFTS ETHICALLY PROBLEMATIC?

Because gifts create relationships, healthcare professionals' acceptance of gifts from the pharmaceutical industry can be ethically problematic in several ways. Accepting gifts risks undermining trust. It may bias clinicians' judgments about the relative merits of different medications. And it may affect prescribing patterns in ways that increase costs and adversely affect access to care.

Undermining Patient and Public Trust

Healthcare professionals' fiduciary, or trust-based, relationship with patients requires that practitioners explain the reasons for treatment decisions and disclose any potential conflicts of interest, including the influence of gifts. One study asked patients and physicians to rate how appropriate it would be for a physician to accept gifts (ranging from pens to trips) from the pharmaceutical industry and whether they thought accepting gifts would influence the physician's behavior. With the exception of drug samples, the patients considered gifts to be more influential than did the physicians. Almost half of the patients who participated had not been aware that physicians received gifts from pharmaceutical companies - and of those, 24% said that this new knowledge changed their perception of the medical profession. Similarly, a telephone survey of patients found that although 82% of respondents were aware that physicians received "office-use gifts" from the pharmaceutical industry, only about one-third were aware that physicians received personal gifts. Forty-two percent believed that personal gifts adversely affect both the cost and the quality of healthcare. On the basis of such data, the American College of Physicians has concluded that "[a] significant number of patients believe that industry gifts bias their physician's prescribing practices and ultimately drive up medical costs." Public awareness that healthcare professionals accept gifts from pharmaceutical representatives may undermine trust in the profession and lead to a perceived loss of professional integrity.

VHA is a public agency and public service is considered a public trust. Consequently, the public rightly hold VHA to a higher ethical standard than they do private companies. As federal employees, health professionals appointed to VHA have an obligation to ensure that citizens can have complete confidence in the integrity of the federal government (5 CFR 2635.101; EO 12674). Whereas the public relies on legal enforcement mechanisms to assure

that private healthcare organizations comply with relevant law and regulation, they expect public agencies and employees to adopt policies that not merely follow the rule of law but also promote its spirit by establishing goals of exemplary behavior as ethical standards. Acceptance of any type of gift from the pharmaceutical industry by VHA employees risks eroding public trust in VHA, possibly to a greater degree than would be the case for employees in private agencies. More importantly, the beneficiaries of government programs—veterans, in the case of VHA—are often more dependent on government services than are those who rely on private programs. This greater dependence gives rise to the government's obligation to adhere to a stricter ethical standard.

Effects on Professional Relationships

Given the ways in which gift giving differs from entering into a contractual relationship, gifts from pharmaceutical representatives to healthcare professionals can blur the distinction between formal business exchanges and informal, interpersonal exchanges. The social experience of giving and receiving gifts affects the relationship between the two parties in complex and subtle ways. Anthropological literature explains that the recipient of a gift often feels three types of obligation toward the giver: grateful conduct (i.e., acceptance of the gift and expression of gratitude), grateful use (i.e., in accord with the giver's intention) and reciprocation. Obligations to accept the gift and thank the giver and to use the gift as the giver intended stem from the purpose of gift exchange - building personal, moral relationships.

The felt obligation to reciprocate, to give or do something in exchange for the gift, is most troubling in the healthcare context. In the context of a gift to a healthcare professional from a pharmaceutical industry representative, practitioners commonly understand that the hoped for reciprocation involves the healthcare professional writing more prescriptions for the drug(s) the representative is promoting.

Bias and Conflicts of Interest

Healthcare professionals may be influenced by accepting gifts in two ways. They understand that prescribing selected pharmaceutical products is the industry's preferred form of reciprocation and some may be influenced to do so in response to the gift received. One study, for example, found that physicians who met with or accepted money from representatives of pharmaceutical companies (e.g., for educational presentations) were more likely to request that the companies' drugs be added to a hospital pharmacy than were colleagues who did not interact with pharmaceutical companies. A review of physicians' prescribing patterns found that usage of two drugs increased significantly among physicians who attended "all-expense-paid" symposia at resorts sponsored by the manufacturer of the drugs compared to their practice before the symposia. The majority of physicians responding did not believe that such incentives would alter their prescribing practices. Similarly, a study reported that British general practitioners who had weekly contact with drug company representatives were more willing to prescribe new drugs and more likely "to express views that will lead to unnecessary prescribing" than general practitioners with less frequent contact with pharmaceutical representatives.

The second concern is that gifts may insidiously introduce undetected or underappreciated bias into professionals' assessment of the overall merit or value of promoted pharmaceutical products. There is evidence to indicate that practitioners themselves are often poor judges of whether or when external factors, such as gifts, influence their decision making. For example, 86% of respondents to a nurse practitioner and physician assistant survey regarding pharmaceutical industry promotions said, "it is appropriate to accept gifts and that these gifts do not influence their prescription choices."

Pharmaceutical industry gifts to healthcare professionals create potential conflicts of interest that can affect practitioners' judgment - without their knowledge and even contrary to their intent - thereby placing professional objectivity at risk and possibly compromising patient care. Trainees may be especially susceptible to conflicts of interest created by gifts. This influence is also detectable among physicians in training and other prescribing professionals. For example, more than half of psychiatric trainees responding to a questionnaire about interactions with the pharmaceutical industry felt that receiving gifts would not influence their prescribing practices. Moreover, "[t]he more money and promotional items a physician-in-training had received, the more likely he or she was to believe that discussions with representatives did not affect prescribing." A study of house staff reported that residents generally do not find gifts from industry problematic and do not believe that they are influenced by them. The study found, however, that residents' behavior was not consistent with their expressed attitudes. For instance, every resident who considered pharmaceutical industry-sponsored conference lunches and pens inappropriate had nonetheless accepted these gifts. Another study reported that the more exposure trainees had to pharmaceutical industry representatives, the higher they rated the general appropriateness of gift acceptance. Yet other research reported that 90% of trainees surveyed acknowledged that pharmaceutical industry representatives in fact were influencing their prescribing practices.

Effects on Healthcare Costs

Gifts from the pharmaceutical industry to healthcare professionals are not "free." The pharmaceutical industry's expenditures for the promotion of prescription drugs, including gifts, are significant, totaling \$15.7 billion in 2000. While healthcare professionals are the beneficiaries of gifts, the cost of these marketing tools is passed through to purchasers and increases the costs of pharmaceutical products in two ways. First, expenditures for gifts are passed

along to consumers in the form of higher prices. Second, if gifts to professionals serve their purpose, practitioners will be influenced to prescribe heavily marketed drugs, which tend to cost far more than less heavily marketed but often equally effective alternatives, such as generic drugs. Data from Great Britain suggest that use of new drugs and higher prescribing costs are “strongly and independently associated” with frequent interactions between healthcare professionals and pharmaceutical representatives. Rising healthcare costs can lead to limitations on access to care.

WHY ARE GIFTS ACCEPTED?

If accepting gifts from the pharmaceutical industry is ethically problematic in these ways, why do healthcare professionals continue to take the pens, textbooks, drug samples, meals and other gifts they are offered? One explanation is that accepting a gift is a natural, socially expected reaction motivated by a combination of self-interest and politeness. But it is also argued that healthcare professionals and trainees have come to expect gifts as part of a “culture of entitlement” that has evolved as a result of years of largesse on the part of pharmaceutical companies. Gifts have become a familiar part of many healthcare workplace cultures and established patterns of behavior often resist change.

Other rationales are that inducements such as free lunches are needed to induce attendance at educational sessions (and may help offset the costs of such programs) and that they help boost employee morale. Some even claim that accepting gifts results in economic savings for healthcare institutions, because the pharmaceutical industry provides for free items that the institutions would otherwise have to buy. Finally, apathy on the part of professional bodies allows the “tradition” of accepting gifts to continue. Failure to enforce ethical standards consistently has made it easier simply not to notice, or not to be concerned about, the fact that accepting gifts creates ethical risks.

None of these arguments, however, is compelling enough to allow an ethically problematic practice to continue. While habit and self-interest can be powerful motivators, ethical standards explicitly require healthcare professionals to place patient interests above their own. The Accreditation Council for Graduate Medical Education (ACGME), which oversees all physician residency programs in VHA, has established important ethical principles to guide relationships with the pharmaceutical industry. One principle is that teaching institutions must ensure that their training programs have sufficient funds from appropriate sources to conduct their educational activities so as to reduce or eliminate the risk of undue influence.

Moreover, any potential cost savings resulting from gifts is likely to be far outweighed by undesirable effects on prescribing practices: gifts influence healthcare professionals to prescribe more expensive medications without a measurable positive effect on patient care, resulting in increased, rather than decreased pharmaceutical costs overall. Moreover the ACGME has concluded that commercially sponsored educational events are far more costly than they need to be.

LEGAL CONSIDERATIONS IN THE VA

In addition to the ethical concerns about acceptance of gifts from pharmaceutical companies, there are legal considerations. Healthcare professionals employed in the VA are subject to federal conduct regulations and conflict of interest laws that do not apply in the private sector. For example, the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635, would prohibit acceptance of gifts from pharmaceutical companies by VA practitioners in most of the situations previously described in this report. Moreover, a VA practitioner may not solicit gifts from a drug company under any circumstance. They also cannot accept a gift in exchange for acting to influence an agency decision, e.g., requesting that a drug be added to the formulary. VA healthcare professionals also cannot accept gifts that result in or appear to involve use of their public office for private gain. For example, if a VA physician were to repeatedly accept a drug manufacturer’s offer to pick up the lunch tab at their regular meetings, it might appear that lunch was being provided in order to reward or encourage that physician to continue recommending the company’s product to VA patients. These and other rules that limit the acceptance of gifts from pharmaceutical companies require interpretation. There is also the potential for criminal as well as administrative sanctions if these rules concerning gifts are violated. Further, practitioners should be mindful of federal statutes governing the area of healthcare fraud and abuse, including the federal healthcare program anti-kickback statute (42 U.S.C. 1320a-7b(b); see also 42 C.F.R. 1001.952). VA healthcare professionals who have questions about legal standards regarding gifts or other interactions with pharmaceutical companies and medical manufacturers should seek guidance from their local Regional Counsel or General Counsel.

HEALTHCARE PROVIDERS' EXPECTATIONS OF INDUSTRY & SALES PERSONNEL

This training module is based on material from the American Medical Association's educational modules on ethical guidelines for physicians' relationships with industry, which may be accessed or downloaded at <http://www.ama-assn.org/ama/pub/category/5689.html>

While a professional sales presentation can be educational, to maintain a balanced perspective, physicians and other healthcare providers must understand the training and background of the industry representative as well as the regulatory expectations that govern the interaction and the provider-industry representative relationship.

ROLE OF AN INDUSTRY REPRESENTATIVE

This section addresses the job, training, accountability and evaluation and compensation of industry sales personnel. Common practices within the pharmaceutical and medical device industry are presented. Within the law, each company may handle specific situations differently as decided by their leadership.

The Job

Industry representatives are responsible for:

- Increasing product sales
- One or more products
- A geographical territory for a group of physicians or for a specific area of health care (e.g., oncology, pediatrics)

Industry representatives also provide disease- and product-specific information to healthcare professionals. The FDA regulates pharmaceutical sales personnel according to their activity, not by title, including prospective visits to physicians' offices and promotional presentations to physicians at group events.

Training

There are no national standards for experience, educational background or training of industry representatives. Some have science or clinical training and most have an undergraduate or graduate degree. Corporate training varies by pharmaceutical manufacturer; many provide an initial six months or more of training such as:

- Three weeks of in-house selling skills training
- Product-related disease training, accompanied by extensive testing
- Drug-specific training

Periodic retraining is also offered as representatives achieve different levels of experience, competency and responsibility. Sales representatives often receive field sales training through calling on physicians accompanied by experienced industry representatives, district sales managers or sales trainers, or through in-office or hospital preceptorships working one-on-one with specialists known for their expertise in specific diseases.

Accountability, Evaluation and Compensation

Industry representatives are assigned a territory (usually a group of zip codes) and are managed by a district sales manager or other similarly titled manager. One or more district managers typically report to a regional sales manager or director.

Representatives are generally required to track the following:

- Samples disbursed (must document under special sampling law)
- Literature left behind
- Any physician questions
- Physician clinical interests/preferences
- Physician interest in giving/attending presentations/events
- Product or disease information discussed
- Plans for next sales call

The evaluation of an industry representative commonly depends on the following factors:

- The number of prescriptions written and/or product sales value for a defined territory
- Sales measured against quarterly data, targets and competitive sales figures
- Information provided during sales calls or requested as a result of a sales call
- Changes in physician-prescribing patterns

Additionally, the evaluation may include :

- The number of sales calls representatives make on physicians, pharmacies, hospitals, etc.
- Calls benchmarked against previous activity and/or targets for the number of daily sales calls

Industry representatives are often paid a combination of salary plus a bonus based on sales goal attainment. They typically are awarded bonuses if they exceed sales goals and may receive other incentives such as trips and luxury items for outstanding performance.

FDA REQUIREMENTS

FDA enforces laws and regulations governing interactions between industry representatives and physicians, including product labeling and package inserts, sales activities and advertising and marketing.

Product Labeling and Package Inserts

For package insert inclusion the FDA requires data from adequate and well-controlled clinical trials that provide independent corroboration of a clinically relevant finding. Anecdotal or testimonial information is inadequate.

Prescription drug approval requires that the demonstrated efficacy/benefit of the product outweigh the known risks of the product for the population for whom the drug is intended when used as described in the label.

Product Information for Sales Activity

Based on the totality of clinical data submitted by the company, the FDA approves the package insert (or "PI", a.k.a "professional labeling" or just "labeling") and the intended use (or "indication" as written in the PI) of the product. Therefore, it is the information consistent with the package insert that the company can legally promote. With a few limited exceptions, such as special accelerated approval for drugs being approved for serious or life-threatening diseases, regulations require manufacturers to submit promotional materials to the FDA at the time of publication or distribution, not prior to use. Therefore, most promotional materials have not been pre-reviewed or approved by the FDA.

According to FDA regulations the manufacturer must ensure that:

- Information about a prescription drug does not mislead
- Anyone acting on their behalf does not mislead by implication
- Prior to FDA approval, promotion does not occur for unapproved products or unapproved uses of approved products
- Information is consistent with the approved PI and truthful and not misleading according to the PI

Industry representatives must:

- Provide safety information about a drug when discussing product attributes and efficacy claims with a physician (called "fair balance")
- Leave a PI with physicians when providing a sales call or printed information on a product

What an Industry Representative Can and Cannot Do

Within FDA regulations, when calling on physicians on behalf of a pharmaceutical manufacturer, a representative CAN:

- As defined in the regulations, provide detailed information that is in the professional product labeling or PI, consistent with the PI or supported by substantial evidence
- Display or distribute company-approved promotional and support materials
- Refer "off-label" questions to the company's medical relations/professional relations department
- Sell using all company-approved material

Within FDA regulations, a representative CANNOT:

- Prompt an "off-label" question
- Discuss product information that is not in the product labeling, PI or company-approved material
- In general, compare the PI of one product with the PI of a competing product, as data are not "apples to apples"

Advertising and Marketing of Off-Label Uses

Industry representatives:

- Can refer physicians' unsolicited off-label questions to their company's medical relations department
- Cannot prompt discussions regarding the use of prescription drugs that is inconsistent with labeling

The pharmaceutical company medical information department will:

- Answer the questions with a narrowly tailored response
- Provide complete reprints (generally not just abstracts) of studies related to the question, even if off-label

- Provide studies that accurately reflect the totality of the known data about that question and not just the most favorable product profile

Paid Speakers

Physicians serving as paid speakers, or otherwise representing a company, are expected to:

- Follow the same promotional regulations as company personnel, since they are acting on behalf of the company (per FDA regulations)
- Be trained by the pharmaceutical company on FDA regulations if they are being paid on behalf of the company (per Pharmaceutical Research and Manufacturers of America [PhRMA] guidelines)

Study Design and Findings

When interpreting study publications and trial data, healthcare professionals should ask themselves the following questions and seek help as needed from biostatisticians:

- Is the study designed to answer the question?
- Is the study adequately powered to answer the question?
- Is the study randomized, controlled, blinded, etc. and does it account for all patients, therefore minimizing bias?
- Do the data support any comparative claims?
- Do the data support the conclusions?
- What are the authors' potential conflicts of interest, financial biases or other personal biases?

FDA regulations do not permit using mechanism of action or in vitro information to support clinical claims or comparisons unless there is proof that these cause clinical outcomes.

Comparative Claims

FDA requirements regarding comparative claims are as follows:

- In general, at least two adequate and well-controlled head-to-head trials are required to support a comparative claim (and/or superiority and "equal efficacy or safety" claims) between two drugs
- (The same applies for product promotion, whether the comparative data are in the label or not)
- Both drugs must be approved for the same indication before a comparative claim can be made

Promotional and Educational Events

Healthcare professionals should be aware of the following differences between an educational event presented by industry and one supported by industry and sponsored by an ACCME accredited organization:

<i>Industry Promotional Education (Non-independent)</i>	<i>Accredited Sponsor Education (Independent)</i>
Funded directly by industry	Often supported by industry through an unrestricted educational grant
Delivered by industry or somebody paid by industry	Delivered by ACCME accredited organization
Content developed by industry	Content developed independently without industry influence
Only company-approved material can be presented and distributed	Not subject to FDA regulation
Regulated by FDA	Off-label discussions permitted if clearly identified as such
Presentations must be consistent with labeling	Speaker selected by accredited sponsor
Speaker(s) usually from industry-approved speaker bureau and trained by the company	Full speaker disclosure required
Not eligible for CME credits	Eligible for CME credits
Sales representatives can promote products consistent with labeling	Industry representatives cannot promote products in same room where education occurs

Quick Case 1: Promotional and Educational Events

You attend a CME activity designated for AMA PRA Category 1 credit by an accredited provider and commercially supported by a pharmaceutical company. At the end of the program, the local industry representative stands up and thanks everyone for coming on behalf of the company. She also states that anyone who would like additional information on the drug discussed in the CME presentation should feel free to contact her.

How appropriate is this conclusion to the program?

- The pharmaceutical representative thanking attendees was clearly at the boundary of acceptable behavior.
- The pharmaceutical representative offering additional information was over the boundary, blurring lines between promotion and education.
- ACCME standards prohibit any behavior that might be construed as sales activities where educational activity occurs.

Quick Case 2: Comparative Claims

An industry representative is making a sales presentation about an antihypertensive drug to a resident physician. The industry representative states, "According to the package inserts for our drug and our biggest competitor, our drug has 5% fewer incidents of cough than their drug."

How should you interpret this statement?

- Comparative claims do not have to be in the labeling, but must be supported by the same evidence as required for a labeling claim. (These trials must involve an approved indication for both drugs.)
- A valid comparison based on two products' respective package inserts is unusual because generally:
 - The trial methodologies, reporting language and endpoints are not identical
 - The trials were not conducted at the same time on the same trial populations
- You should ask to see results of a head-to-head trial.

PROVIDER RESPONSIBILITY

This section addresses physicians' and other providers' responsibility in reporting safety issues regarding prescription drugs and violations of promotional activity, as well as VA policies on pharmaceutical sales representatives and sampling.

Safety Alerts

At NYHHS all adverse events, including those related to medications, are to be reported on a Patient Incident Report (VA Form 10-2633). The event should be documented in the progress notes and include what occurred, the results of the evaluation and necessary treatment. No mention of the 10-2633 may be made in the medical record. All adverse events must be discussed with the patient and his family. The attending physician with concurrence of the Executive Chief of Staff is responsible for informing the patient and his family about injuries resulting from adverse events and the compensation options available to them.

Promotional Concerns

Physicians and other healthcare providers should report industry representative violations of promotional activity regulations to:

- The responsible company's medical information department
- The FDA's Division of Drug Marketing, Advertising and Communications within the Center for Drug Evaluation and Research, 5600 Fishers Lane, HFD, Rockville, Maryland 20857, telephone: 301-827-2828 or 301-827-2831 / fax: 301-594-6759 or 301-594-6771, <http://www.fda.gov/cder/ddmac/>
- HHS, Office of the Inspector General; telephone 1-800-447-8477

VA Policy on Pharmaceutical Sales Representatives and Sampling

VA healthcare providers, house staff and students must follow VISN 3 and facility policies covering pharmaceutical sales representatives and sampling. These policies include the following requirements:

- The use of drug samples for patient care is not authorized. Samples for personal use cannot be sent to or kept in the facility.
- If a physician or other provider is interested in using a drug or medication, the drug must be approved by the Pharmacy and Therapeutics Committee and the sample must be dispatched to the Pharmacy Service for distribution.
- Pharmaceutical sales representatives must have a scheduled appointment to enter the facility. Appointments with residents and interns may be made only after obtaining the approval of the VA service chief.
- Employees, residents or students may not solicit or accept any gift, gratuity, favor, entertainment, loan or anything of monetary value from a pharmaceutical sales representative or any other person seeking or involved in a financial relationship with the VA.
- Vendor representatives are prohibited from providing refreshment of any sort in any amount to any VISN 3 employee, resident or student either on or off site.

MANDATORY TRAINING TEST

Name (Please print): _____

Date: _____

Social Security No. (last 4): _____

Service: _____

Directions: Mark your answer to each of the following questions and SIGN the certificate following the test.

INFECTION CONTROL

1. Hand hygiene is considered the most important infection control measure.
True False
2. Standard Precautions means treating all blood and body fluids as if they were potentially infectious.
True False

FIRE PREVENTION

3. PASS is:
 - A. An information sheet with OSHA required chemical information
 - B. An easy way to remember how to use a fire extinguisher
 - C. The proper technique for evacuating patients
 - D. None of the above
4. RACE stands for:
 - A. Rescue, Alarm, Contain, Extinguish
 - B. Run and Call Engineering
 - C. Rescue, Apprehend, Cuff, Escape
 - D. Ready, Aim, Count, Extinguish

HAZARDOUS MATERIALS

5. All chemicals must have a label on them, even if the container is not original.
True False
6. The chemical inventory and MSDS are located in the GREEN Safety Manual.
True False

GENERAL SAFETY

7. Smoking is permitted anywhere in this facility.
True False

UTILITIES SYSTEMS

8. Outlets on emergency power are either colored orange or labeled "emergency power."
True False

EMERGENCY MANAGEMENT

9. The Emergency Management Manual is:
- A. Green
 - B. Yellow
 - C. Red
10. In the event of an evacuation from a patient care area, the first course of action should be:
- A. Move patients outside of the building
 - B. Move patients to the Emergency Department
 - C. Move patients horizontally, then to a lower floor, if needed
 - D. Move patients to the area of the fire

SECURITY MANAGEMENT

11. When you access data on another employee in the computer system, no one knows but you.
True False

WORKPLACE VIOLENCE AWARENESS & PREVENTION

12. Which of the following actions should you take to prevent or deal with workplace violence?
- A. Wear your ID badge.
 - B. Be supportive of those who have experienced workplace violence.
 - C. Call code 4000 if you witness violent or uncontrolled behavior.
 - D. All of the above.
 - E. A and B only.

OCCUPATIONAL HEALTH

13. If you are injured on the job, you must report to Employee Health or the Emergency Department with your supervisor.
True False

GEMS

14. A GEMS pollution prevention initiative includes the recycling of:
- A. Paper
 - B. Soda bottles and cans
 - C. Ink cartridges
 - D. All of the above

INFORMATION SECURITY AWARENESS

15. Breaches in confidentiality may occur when:
- A. You walk away from your computer without properly signing out
 - B. Patient care issues are discussed in public areas
 - C. Printouts with sensitive information are not properly controlled
 - D. All of the above
16. What should you do if you receive an e-mail attachment from someone you don't know?
- A. Do not open the attachment.
 - B. Open the attachment if the subject line seems appropriate.
 - C. Reply to the e-mail and request more information.
 - D. Open the attachment if your virus software doesn't alert you not to.

SEXUAL HARASSMENT & THE DISCRIMINATION COMPLAINT PROCESS

17. What form of sexual harassment is shown in the following situation? A supervisor tells his secretary that if she goes to a hotel with him after work he would see to it that she gets a promotion.
- A. Hostile work environment
 - B. Quid pro quo
 - C. Sexual favoritism

PATIENT SAFETY PROGRAM & PERFORMANCE IMPROVEMENT

18. When giving a medication to a patient, you should be sure to state the patient's name as assurance that you are giving it to the correct person.
True False
19. The PDCA cycle refers to the process of Propose, Decide, Comply, Assess.
True False

PAIN MANAGEMENT

20. A patient's self-report of pain intensity is the most reliable measure of pain.
True False
21. Pain Intensity Rating scales are found at nursing stations only.
True False

GIFTS TO HEALTHCARE PROVIDERS FROM THE PHARMACEUTICAL INDUSTRY

22. A healthcare provider in the VA system should not accept a gift from a pharmaceutical sales representative for which of the following reasons?
- A. The provider may feel obligated to reciprocate by increasing the number of prescriptions of drugs promoted by the company.
 - B. Acceptance may create a bias toward the company's drugs, undermining patient care decisions and trust.
 - C. Gift giving by drug companies increases healthcare costs which can restrict access to care.
 - D. All of the above.
23. A VA healthcare provider may not solicit a gift from a pharmaceutical sales representative under any circumstance.
True False

HEALTHCARE PROVIDERS' EXPECTATIONS OF INDUSTRY & SALES PERSONNEL

24. What is the FDA's requirement for prescription drug approval?
- A. Efficacy superior to a placebo
 - B. Efficacy superior to any other agent in its class
 - C. Efficacy and benefit outweigh the known risks for the intended population
 - D. All of the above
25. Which of the following are required by FDA to support a comparative claim between two drugs by a pharmaceutical company in its advertising and marketing activity?
- A. One adequate and well-controlled trial
 - B. In general at least two adequate and well-controlled trials
 - C. Approval of both drugs for the same indication
 - D. A and C only
 - E. B and C only

CERTIFICATE OF TRAINING

I have read all the training modules included in NYHHS's Mandatory Training Manual 2009-2010, including the print version of the VHA Privacy Policy training and confirm that all information has been understood.

I have read the module on VHA Compliance and Business Integrity (CBI) Program and understand the purpose of the CBI Program and the Ethical Standards of Conduct.

Print Name: _____

Date: _____

Signature: _____

Campus: _____

Service: _____

Complete, sign and return this test and certificate (pages 61-64) to NYHHS by fax or mail to your contact individual following the instructions provided with transmittal. THANK YOU!