

Student Orientation



WELCOME

Welcome to Yakima Valley Memorial's student on-boarding experience.

We are pleased that you chose to join us!

We are a mission, vision and values driven provider of exceptional quality service. During our history as a community hospital, we have played a significant role in enhancing the quality of life in the Yakima Valley.

You will be working with a team of engaged colleagues who do amazing work...*every day!* We focus upon creating the healthcare experience of choice for our patients and customers, and we look forward to creating an exceptional experience for you as well.

Required Topics

- Yakima Valley Memorial Info
- Safety
- Emergency Preparedness
- Infection Control
- Blood borne Pathogens
- Patient Safety
- Patient Rights
- Cultural Diversity
- Workplace Violence
- Harassment
- Acceptable Use
- Privacy and Confidentiality-HIPAA
- Integrity Program
- Standards of Conduct

Core Purpose

To inspire people to thrive

Vision

Creating healthy communities one person at a time

Mission

Achieving health with you in new ways

Values

Respect*Accountability*Teamwork*Stewardship*Innovation



Parking

- We have designated parking areas/lots at each Yakima Memorial facility for our safety and convenience.
- Students are to park in any designated employee area (see next slide). No permit is required.
- Parking lots are monitored! Please make sure to park in designated employee areas.



Memorial Campus Map



Non-Smoking Work Environment & Substance Abuse

Yakima Valley Memorial and its family of services are smoke free environments. Employees, students, and volunteers may smoke in your personal vehicle in employee parking lots.



Yakima Valley Memorial recognizes responsibility to maintain a work place that is safe, healthful and productive. The possession, dispensing, or use of alcohol or illegal drugs, or the abuse of legal drugs is prohibited.

Appearance & Dress Code

- Badges: Wear your school *and* Yakima Valley Memorial issued badge at all times during your scheduled shift. No slogans, pictures, advertisements, and/or other materials may be placed on a badge or its attachments
- Hygiene: Please maintain an acceptable level of cleanliness, which includes:
 - Wearing deodorant
 - Remain odor neutral; no fragrances are to be worn
- Dress Code: Depending on your position, you may wear scrubs or business casual (no jeans)
- Footwear: Depending upon your position, your manager may ask you to wear or refrain from wearing specific kinds of footwear. Please ask your manager



Clothing and Accessories

Please refrain from wearing the following while on your shift:

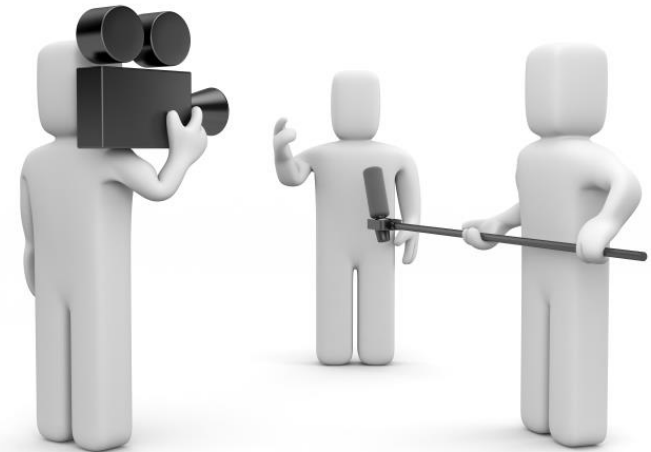
- Facial or tongue jewelry
- Ear lobe expanders
- Sweatshirts, tank tops, miniskirts, and jeans
- Flip flops. Note—closed toed shoes and socks or stocking are to be worn if assigned to a clinical area
- Cologne, perfume, or aftershave lotion. Make-up should be used moderately
- Political pins, religious or holiday pins
- Artificial nails of any kind. Fingernails are to be trimmed short; if nail polish is worn, it must be in good repair
- Any tattoos must be covered, unless unsafe to do so
- Refrain from chewing gum while on your shift



Media Relations

Because Yakima Valley Memorial enjoys a strong presence in the community, there are times when members of the media may be in the hospital or one of our facilities.

Any interviews or inquiries from the media (radio, television, print, or internet) are to be referred to the Marketing and Communications department.



Non-Solicitation

Yakima Valley Memorial prohibits solicitation by, and of, its employees, contract staff, volunteers, and students (collectively, individuals), except as expressly set forth in the policy.

Solicitation on our premises by visitors is prohibited, unless expressly otherwise stated in this policy.



The Patient and Family Experience

At Yakima Valley Memorial, we promote and support a work environment that assists our staff and students in providing a *superior* patient and family experience.

Why is the *Patient/Family Experience* so important?

- Providing a quality patient/family experience shows respect and compassion.
- Patients are demanding a more customer-friendly experience
- Better experience equates to a safer patient care

**Key words used by Yakima
Valley Memorial Staff:**
A.I.D.E.T.

Acknowledge
Introduce
Duration
Explanation
Thank You



Incidents & Injuries

- If you are involved in an unusual incident relating to patients, personnel or visitors, or you are injured, please report the incident immediately to your supervisor.
- If you are injured while on duty, inform your supervisor. Your supervisor will direct you where to proceed for treatment.



Safety

OSHA's Categories of Hazards



Hazard Category	Definitions	Examples	Safe Guards
Biological	"Germs"	HIV, VRE, MRSA, HBV, HCV, TB	Infection control (hand hygiene, PPE [glossary], etc.)
Chemical	Toxic or irritating materials	Detergents, solvents, disinfectants, sterilizing, agents, waste anesthetic, gases, hazardous drugs, mercury	Engineering controls, work practice controls, PPE
Psychological	Factors that cause emotional stress or strain	Working with terminally ill patient, patient deaths, overwork, understaffing, tight schedules, equipment malfunctions	Stress management, relaxation exercise, meditation
Physical	Agents that can cause physical harm	Radiation, lasers, noise, electrical equipment, extreme temperatures	Dependent on hazard
Environmental and Mechanical	Factors that increase risk of accident, injury, strain, or discomfort	Lifting and moving patients, tripping hazards, poor air quality, slippery floors, clutter	Maintenance of a safe work environment, prompt reporting of hazardous conditions

Proper Lifting & Moving Techniques



- Size up the load. If the object is too heavy, large or awkward, get help
- Put your feet close to the object and about shoulder width apart
- Bend your knees, not your back. Use your large leg muscles to do the work
- Keep the object as close to your body as possible

Preventing Slips

- Keep floors clean and dry
- Increase the friction of floors with abrasive coatings, nonskid strips or rubber mats
- Secure rugs with skid-resistant backing
- Choose slip resistant shoes. Look for: soft rubber soles, a large amount of surface area in contact with the floor (no heels) and patterned soles that increase friction
- Post safety signs around slip hazards (icy sidewalks, wet floors, etc.)

If you witness or experience a safety event, please report to the nearest employee and your manager!

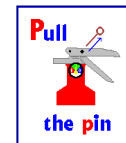
Fire Safety

RACE

- **R - Rescue** anyone in the immediate area
- **A - Activate** the fire alarm pull box
Notify the switchboard:
Hospital- Dial 8123
Offsite-Dial 911
- **C - Contain** the fire by closing doors and windows
- **E - Evacuate**
 - 1st-Evacuate rooms in the danger zone
 - 2nd-Evacuate rooms next to fire
 - 3rd-Evacuate rooms directly across from fire
 - 4th-Evacuate all other rooms left in fire proximity
- **Do not use elevators unless authorized by Fire Department!**

How to use a Fire Extinguisher—PASS!

- P - Pull** the safety pin out
- A - Aim** the nozzle at the base of the fire
- S - Squeeze** the handles to start the foam dispensing
- S - Sweep** the extinguisher from side to side



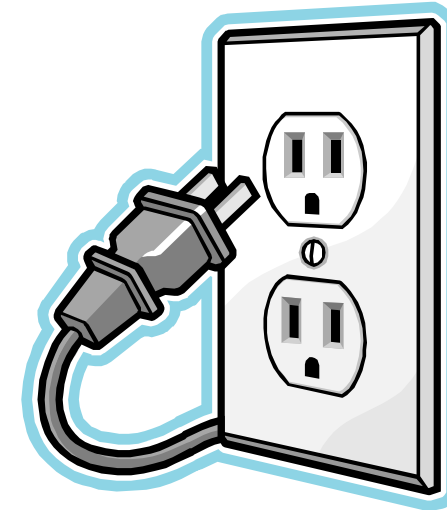
Safety

- To aid in the safety of everyone, *know the location of the nearest*
 - **Fire extinguisher**
 - **Alarm pull box**
 - **Primary & secondary evacuation routes** in your assigned area.
- If you see a **SPILL**
 - **Mark and Isolate**
 - Call Environmental Services at ext. 8049



Electrical Safety Tips

- Use the plug end part of the cord to unplug any appliance
- Report all damaged cords and outlets to Facilities Management
- Facilities must check any equipment being brought in from outside
- If you have an electrical Safety Concern, please contact Facilities Management



Facilities Management ext. 8052
or (509) 575-8052

Infection Control

HAND HYGIENE IS THE MOST IMPORTANT ACT FOR INFECTION CONTROL

Hand Washing Procedure: When washing hands with soap and water, wet hands first with warm water, apply a generous amount of foam soap, and rub hands together vigorously for **at least 15 seconds**, covering all surfaces of the hands, fingers and wrists. Rinse hands with water and dry thoroughly with a disposable towel. Use a dry disposable towel to turn off the faucet. Avoid using hot water, because repeated exposure to hot water may increase the risk of dermatitis.

When in doubt: Treat all bodily fluids as though they pose a potential risk for infection and avoid direct skin contact with them!

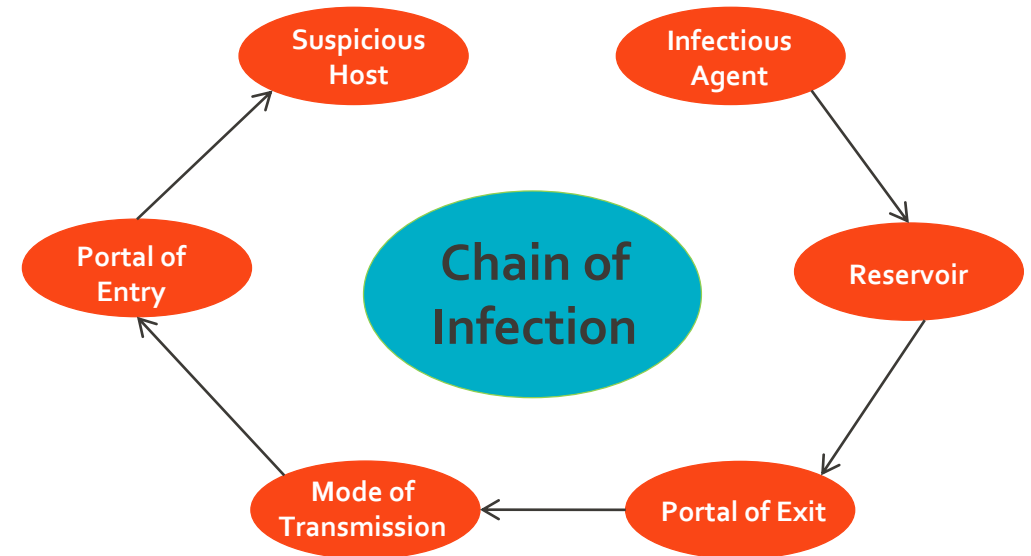


Infection Control

- Students with an active, infectious disease or process are **not** to report to their shift. Notify your instructor and your assigned department/preceptor that you will not be at your shift.

Report active or infectious diseases to:

- Preceptor or supervisor of your assigned area
- Employee Health Services



Blood Borne Pathogen Exposure

In the event of an exposure **YOU** should follow the **WIN** acronym

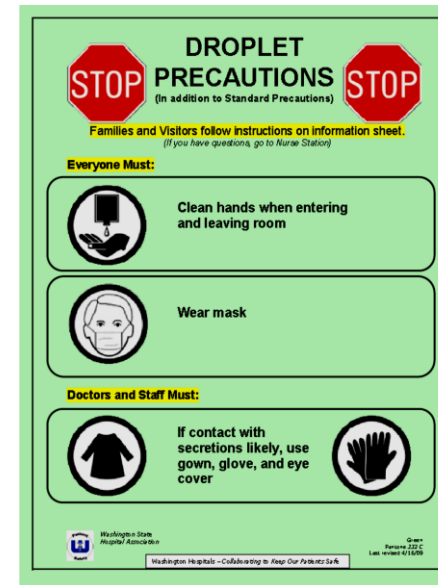
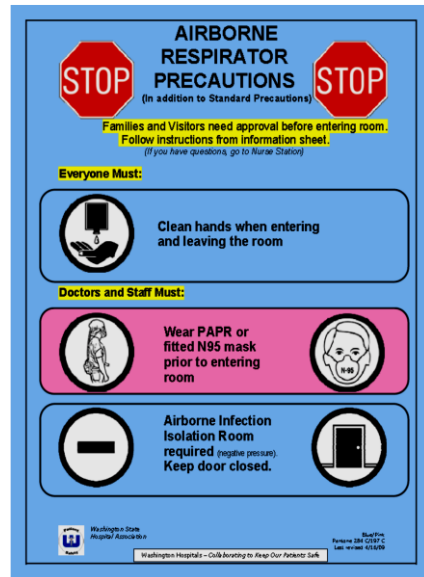
- W** Wash the area with soap and water
- I** Identify whose blood you were exposed to
- N** Notify your supervisor

Your preceptor or supervisor will instruct you where to go for follow-up after an exposure.

Use Standard Precautions whenever you may have contact with patient blood, body fluids, secretions, and excretions.

Precaution Rooms

Do not enter a patient room that has precaution signs without first checking with your preceptor. In many cases, protective clothing is required to enter these rooms.



HIV/AIDS

HIV is one of the most important health threats of our time.

All healthcare professionals need a basic understanding of the virus (HIV) and the disease (AIDS) caused by the virus.



HIV and AIDS are **NOT** the same!

- HIV is a virus that affects the human immune system (Human Immunodeficiency Virus)
- AIDS is the disease that the virus can cause (Acquired Immune Deficiency)

HIV/AIDS Important Points:

- HIV is found in blood, semen, vaginal secretions, and breast milk.
- HIV can be spread through high-risk behaviors. This includes unprotected sex and sharing injection-drug equipment.
- An HIV-positive mother can spread the virus to her child during pregnancy, labor and delivery, or breastfeeding.
- Healthcare workers are at risk for occupational exposure to HIV (needle-stick or other sharps injury, splashes, sprays, or other sources of patient bodily fluids).
- Many bodily fluids do not contain HIV (sweat, saliva, tears).
- HIV cannot be spread through casual contact (shaking hands, hugging).

In addition, a person cannot get (or give) HIV infection from:

- Clothing
- Public drinking fountains, phones, or toilets
- Sharing a meal
- Insect bites or stings
- Donating blood
- Kissing with closed mouth



HIV Exposure – Reducing Your Risk

To help protect workers from HIV and other blood borne infections, the Occupational Safety and Health Administration (OSHA) issued the Blood borne Pathogens Standards (BPS). The BPS mandates the use of Standard Precautions. According to Standard Precautions, healthcare workers should:

- Assume that all blood and other bodily fluids are infectious
- Use barrier protection (gloves, face shield, protective clothing, etc) as needed to protect skin and mucous membrane from contact with blood or other bodily fluids
- Wash hands and other skin surfaces immediately and thoroughly after contact with patient blood or other bodily fluids
- Wash hands immediately after glove removal
- Avoid accidental injury from needles, scalpel blades, and other sharps

Patient Safety

Everyone has a role in patient safety and everyone can benefit from its success!

Do you have a patient safety issue or concern?

Contact your preceptor, instructor, or nurse manager



Joint Commission National Patient Safety Goals

The purpose of National Patient Safety Goals is to improve patient safety. The goals focus on problems in health care safety and how to resolve them

- Identify patients correctly
- Improve staff communication
- Medication Safety
- Alarm Management
- Infection Prevention
- Identify patient safety risks
- Prevent mistakes in surgery



Placing multiple barriers (technology, processes, and people) designed to stop active errors.

Pay attention to Detail: Self Check using STAR



Stop -- Pause for one second to focus attention on the task at hand

Think -- Visualize the act and think about what is to be done

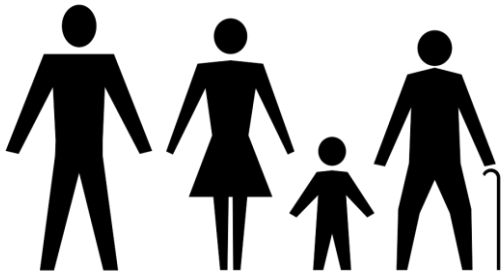
Act -- Concentrate and perform the task

Review -- Check for the desired result

Self Check

The most effective way to avoid slips and lapses. It only takes a second to do and reduces the probability of making an error by a factor of 10 or MORE!

Patient Rights



- Access to care/Healthcare Information
- Be treated with dignity and respect
- Pain Management
- Informed and be involved in all aspects of care
- Protection from abuse and neglect
- Receive information in a manner that meets your needs
- Safe care

The Joint Commission Standards State:

- The patient has a right to, and receives care that is considerate and respectful of his or her personal values and beliefs.
- The assessment of patients considers not only physiological status, but also psychological and social concerns
- A patient's cultural and family contexts, and individual background are important factors in response to illness and treatment.



These standards require:

- Staff to support the patient's expression of value and beliefs, within the limits of our mission and philosophy
- The patient to be allowed to exercise cultural and spiritual beliefs that do not interfere with the well-being of others or the planned course of medical therapy for the patient
- Patient care to demonstrate awareness of the spiritual aspects of patient care



Patients are the Most Important Part of Our Work

*They are the incentive that directs us through the day.
They are our purpose, and their care and comfort deserve first priority.*

***As a student at Yakima Valley Memorial, your
responsibilities include:***

1. Respecting patient confidentiality and privacy
2. Extending courtesy to all visitors, patients, and staff
3. Offering assistance whenever you see someone in distress, lost or confused
4. Promoting a positive work environment to your fellow students and staff
5. Following safe practices at all times



Diversity: Differences that Make Us Unique

- Appearance
- Ethnicity and Culture
- Age
- Religious, spiritual or Philosophical Beliefs
- Income/Social Status
- Sexual Orientation
- Physical/Mental Abilities
- Life Experiences
- Educational Background



Cultural Sensitivity

Understanding, respecting, and valuing physical, cultural, and social differences among individuals

YVM INTERPRETER SERVICES

Dial 8274

OR 575-8274



Cultural Sensitivity

- Focus on the person
- Appreciate their complexity
- Lead with respect
- Honor differences
- Listen to what they need rather than share what you believe
- Learn about them
- Offer best care



Considerate and Respectful Care

- Each patient deserves considerate, respectful care which recognizes and maintains their personal dignity
- In maintaining patient dignity, remember to allow personal expression, and to attend to emotional, social and spiritual needs of the patient and family

If you think a patient's privacy rights have been violated or a patient has questions regarding confidentiality:

- Call the Integrity Hotline at 1-877-684-8658
or
- Call the Patient and Family Experience Department at 509-469-5411

Workplace Violence

- **CODE GRAY:** An emergency response to out-of-control patient, visitor, or staff. Behavior that presents a threat to self or others.

Initiating a Code Gray:

- Dial 8123
- Inform operator-Code Gray and area/room number

CODE SILVER: Active shooter or person brandishing a weapon (imminent threat)

If you are in an active shooter situation, your order of response should be **RUN-HIDE-FIGHT**

- Dial 911 (if safe to do so)
- Dial 8123-inform operator of Code Silver

YVM has trained security. Should you need help, you may contact them at (509) 494-7233 or ext. 7233 (SAFE)



Code Silver Responses

1. RUN	2. HIDE	3. FIGHT
<input type="checkbox"/> Leave personal belongings behind.	<input type="checkbox"/> Find a place to HIDE. Remain silent.	<input type="checkbox"/> Only if your life is in imminent danger, should you attempt to incapacitate the shooter.
<input type="checkbox"/> Do not run through a long hallway to get to an exit.	<input type="checkbox"/> Lock doors if door locks available.	<input type="checkbox"/> Actions should be applied with committed force or aggression in order to be effective
<input type="checkbox"/> Be aware of your environment and take note of nearest exits.	<input type="checkbox"/> Barricade the doors by any means available (furniture, cabinets, beds, equipment, etc.).	
<input type="checkbox"/> Evacuate. Avoid elevators. If escape is not possible – then HIDE.	<input type="checkbox"/> Close and lock windows. Close blinds or cover windows	<input type="checkbox"/> Only attempt to incapacitate a shooter if no other options remain.
	<input type="checkbox"/> Turn out the lights.	
Take others with you. Do not stay behind because others will not go.	<input type="checkbox"/> Silence <u>all</u> electronic devices. Turn off the sound & vibration to cell phones.	<input type="checkbox"/> Identify and improvise weapons which may be thrown to distract, disarm and/or seriously injure the shooter.
<input type="checkbox"/> Do not attempt to establish contact or negotiate with the suspect(s).	<input type="checkbox"/> Remain in place until given an “All Clear” by identifiable law enforcement or “All Clear” announcement.	
<input type="checkbox"/> When safe to do so – CALL 911. Remain on the line with 911 if safe to do so.	<input type="checkbox"/> If two or more individuals seek shelter in the same location, do <u>not</u> huddle together. *Hide along wall closes to exit but out of view from hallway.	
<input type="checkbox"/> When Safe to do so – Dial 8123. Provide clear & accurate information.	If you are unable to evacuate or hide, then FIGHT.	

Harassment

Title VII of the Civil Rights Act of 1964 defines sexual harassment as: “unwelcome *sexual* advances, requests for *sexual* favors, and other verbal or physical *harassment* of a *sexual* nature.” Harassment can be non-sexual and based off of factors such as race, religion, age, disability, origin, etc.

To work toward
eliminating
harassment in your
facility:

If you are a victim,
confront the harasser
directly and make
them aware that their
conduct is
unwelcomed, if you
feel able to do so

If you witness or are
a victim of
harassment or
discrimination,
report it to your
preceptor, instructor,
nurse manager, or
student experience
specialist

Acceptable Use of YVM Information Systems

What Responsible Use Supports (Overview)



Internet Security

Safe and responsible use of the Internet for work related purposes.



Email Security

Using email in a manner that is safe, thwarts phishing attempts, and protects confidential information.



Network Security

Protection of Virginia Mason Memorial's network and systems against hackers and unauthorized access.



Data Protection

Ensuring that Virginia Mason Memorial's data and confidential information is protected, and only accessed by those needing it to do their job.

Acceptable Use

What Responsible Use Supports (Overview)

T



Accessing and using Virginia Mason Memorial devices and networks appropriately for work, and in a way that does not expose Virginia Mason Memorial to security risks.



Adherence to Virginia Mason Memorial's Social Media policy which supports using social media in a way that does not make it appear that you are speaking for Virginia Mason Memorial, and in a manner that protects Virginia Mason Memorial's reputation.

Acceptable Use -- Enforcement

- Compliance with Yakima Valley Memorial Acceptable Use policies is not a suggestion, it is required by Yakima Valley Memorial and some laws.
- “I didn’t know” does not excuse a violator from disciplinary action.
- Violation(s) may result in:
 - Disciplinary action including termination of computer privileges
 - Termination of internship or rotation
 - Legal penalties
 - Fines



YVM Information Systems

- Your use of devices and media can directly impact YVM's reputation, regulatory compliance, and ability to care for patients.
- Only the Yakima Valley Memorial Information Systems department is authorized to approve, install, configure, or alter devices, systems, and software.
- Even if you believe you have the skills required, you are not authorized to approve, install, configure, or alter devices, systems, and software.
- Only YVM managed devices are authorized to be connected to YVM's wired network.

Information Systems Help Desk: (509) 575-8175



Mobile Phones, Devices, and Cameras

- Your devices must be stored out of public view in areas with patient interaction.
 - Use off-duty time for personal calls or text messages
- Non-Yakima Valley Memorial devices must not be used for photography of Protected Health Information (PHI) under any circumstance.
- Your devices must not contain proprietary information or images of current or former patients or workforce members.
- Never text PHI from your personal device or in an unsecured application.



Other Prohibited Actions

Saving non-work related files to our systems.

Attempting to download unauthorized programs.

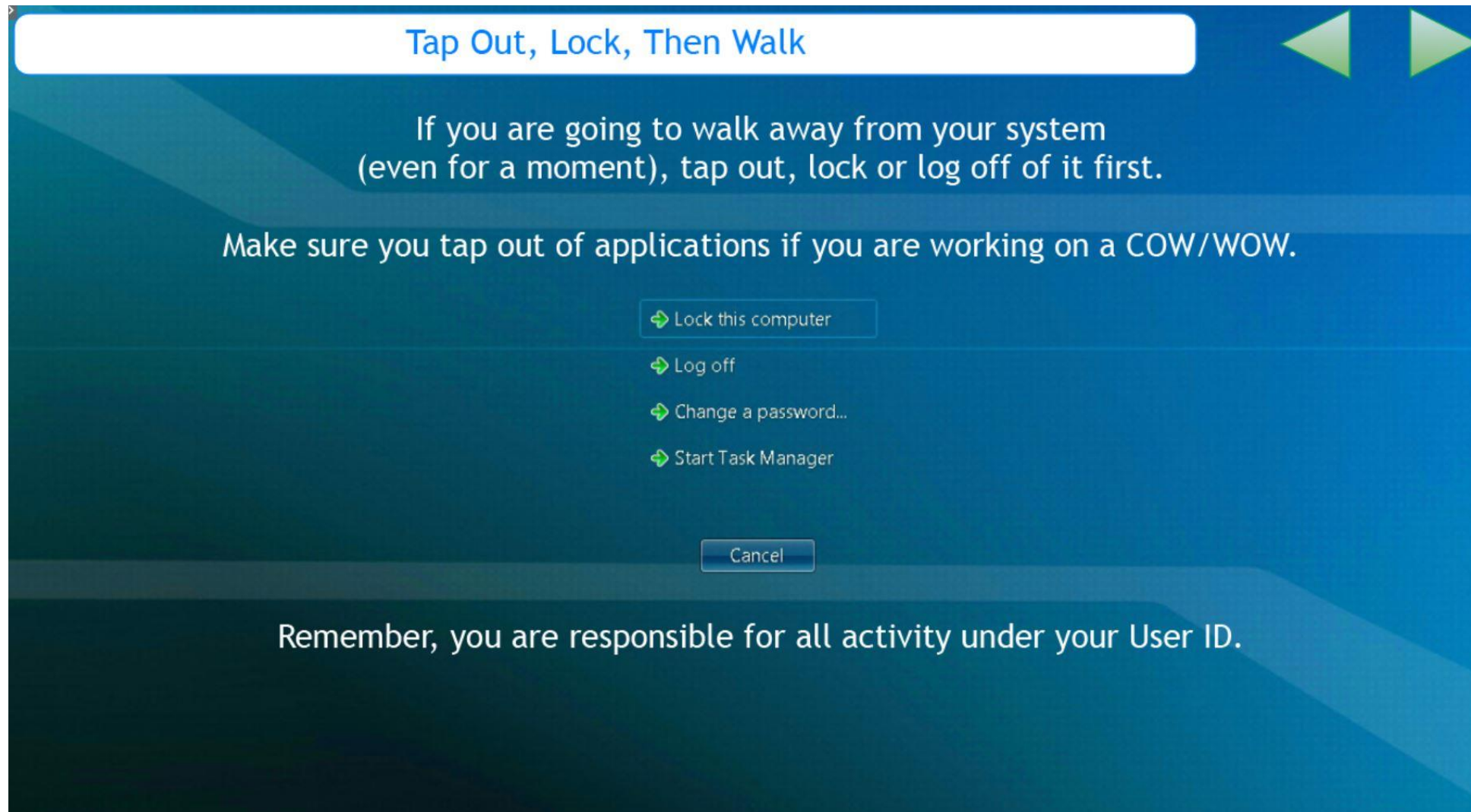
Attempting to download files or documents from the Internet without being sure of their security and/or authenticity.

Attempting to disable Virginia Mason Memorial's antivirus controls.

Attaching devices not approved by Information Systems, including printers, external drives, routers, switches/hubs, etc.

Using a personal email account for business use.

Best Practices



Tap Out, Lock, Then Walk

If you are going to walk away from your system (even for a moment), tap out, lock or log off of it first.

Make sure you tap out of applications if you are working on a COW/WOW.

- ➡ Lock this computer
- ➡ Log off
- ➡ Change a password...
- ➡ Start Task Manager

Cancel

Remember, you are responsible for all activity under your User ID.

Never Share Login Information

- DO NOT....
 - **Share passwords with anyone.** This includes other students, employees, or Information Systems team members.
 - **Let others use your login.** If a student or employee does not have the access they need, they need to contact their supervisor.
 - **Call the Help Desk to request a password reset for another student or employee.** This is a policy violation.

Information Systems will never ask you for your password.



Protecting Patient Privacy

Basic Terms and Definitions



Confidential Information

Confidential information includes any information (oral, written, electronic) that identifies a patient. This includes health, financial and demographic information. Examples include:

- Patient Name
- Medical Record Number
- Social Security Number
- Address
- Date of Birth
- Diagnosis
- Medical History
- Medications
- Credit Card Information

Protected Health Information

Protected Health Information (PHI) is individually identifiable health information in any form (paper, electronic or oral).

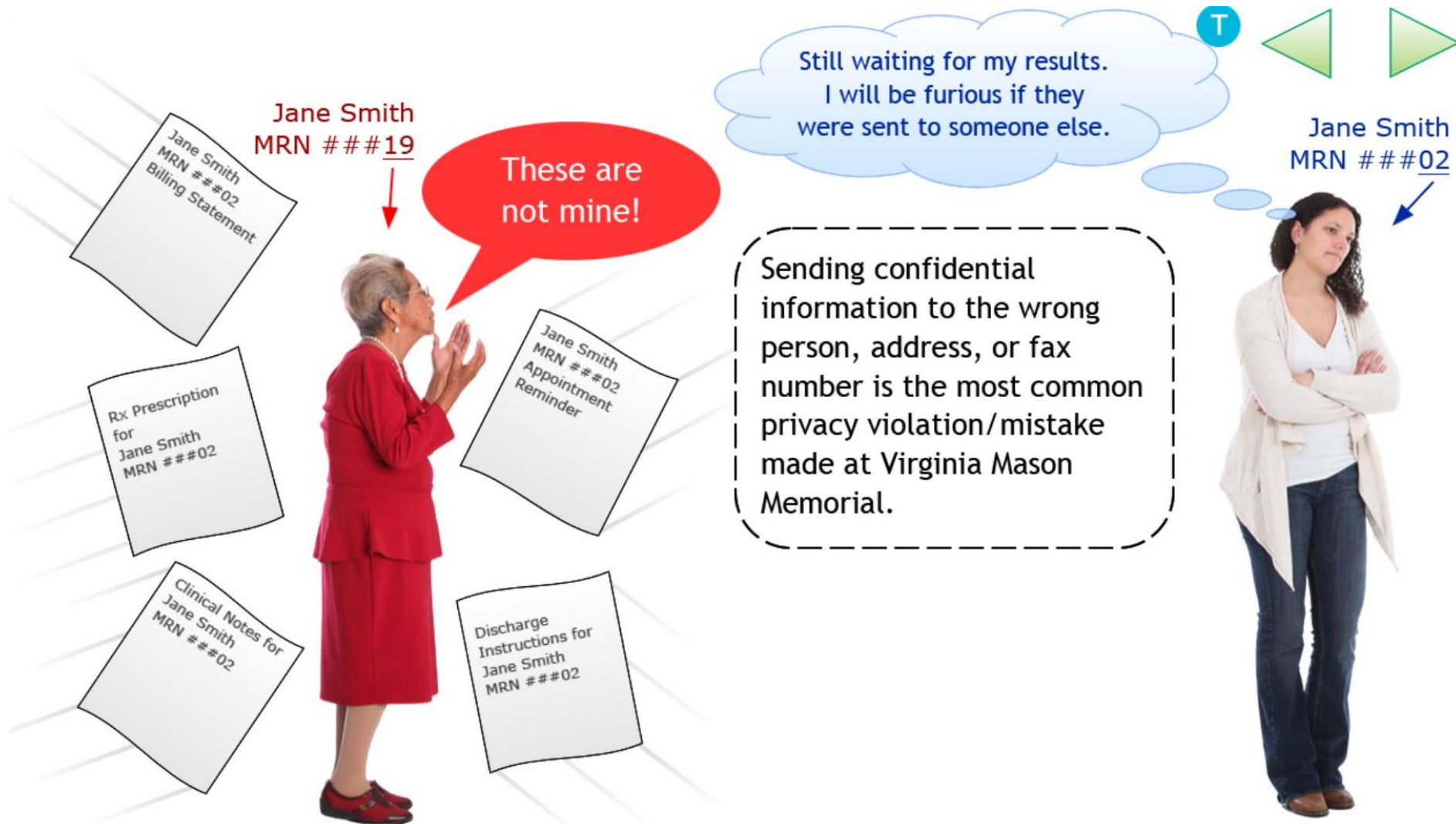
PHI is confidential and must be protected.

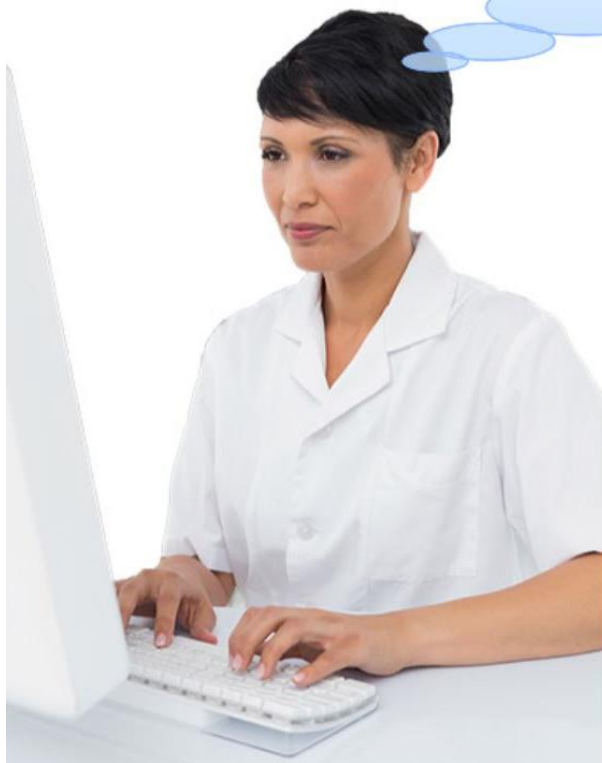
Protecting Patient Privacy -- HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) is a privacy rule that creates national standards to protect individuals' personal health information (PHI) and gives patients increased access to their medical records.
- A breach is the acquisition, use, or disclosure of PHI, in a manner not authorized by HIPPA which compromises the privacy or the security of PHI.
 - It doesn't matter whether a breach is intentional or unintentional.

Health
Insurance
Portability
Accountability
Act







The patient that John is caring for down the hall seems interesting. I think I will look at that record. The patient is on our unit, so I am allowed to access it.



NO! This is a violation.

You are always on a need to know basis:

If you are not part of the care team or providing services to a patient as part of your job, then you are not allowed to view that patient's information. Even if they are being seen in your area.

You must access the minimum necessary:

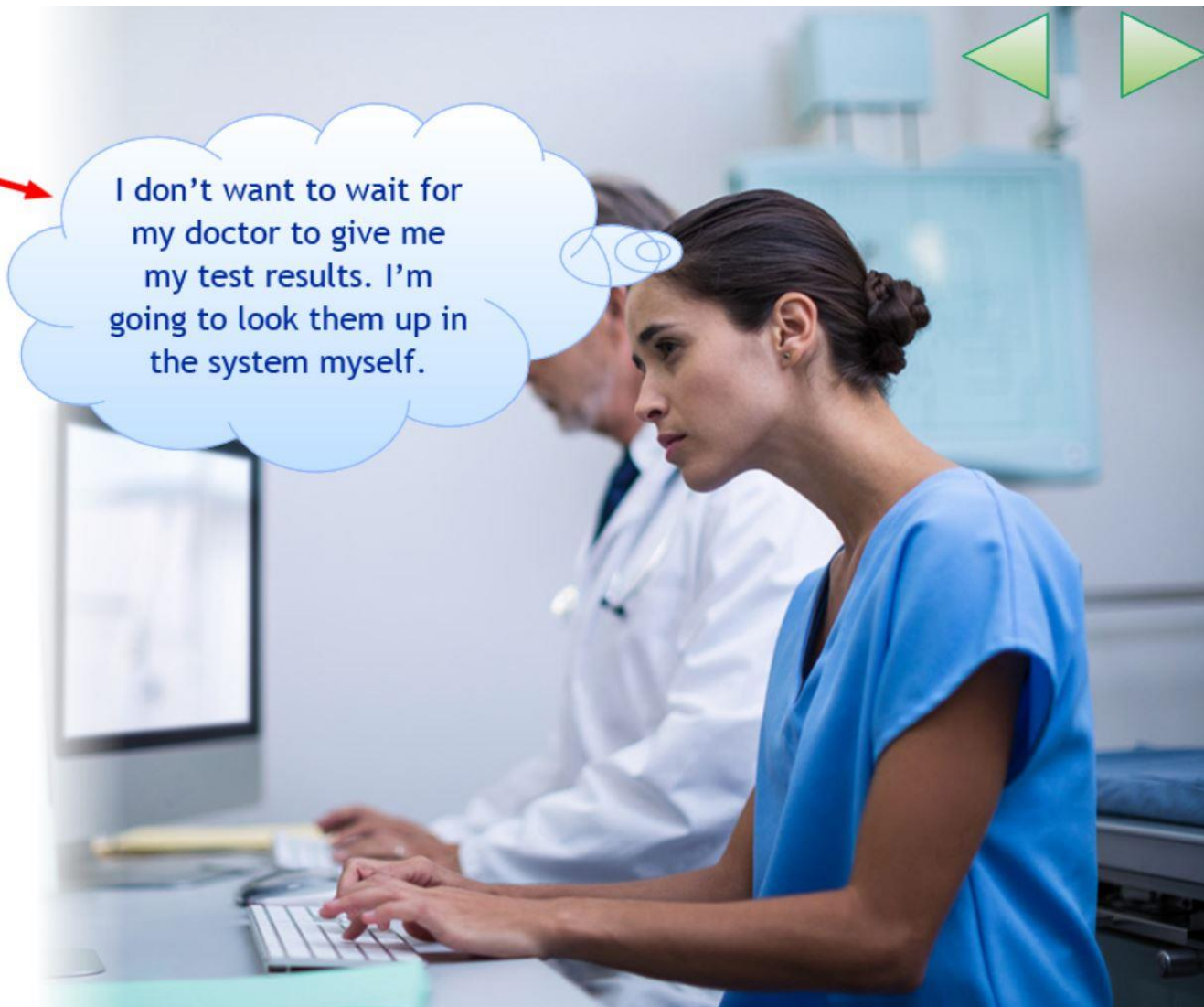
Access of PHI must be the minimum necessary to perform your job.



This is a violation.

You **MUST NOT** access information about anyone unless it is required to perform your job. This includes:

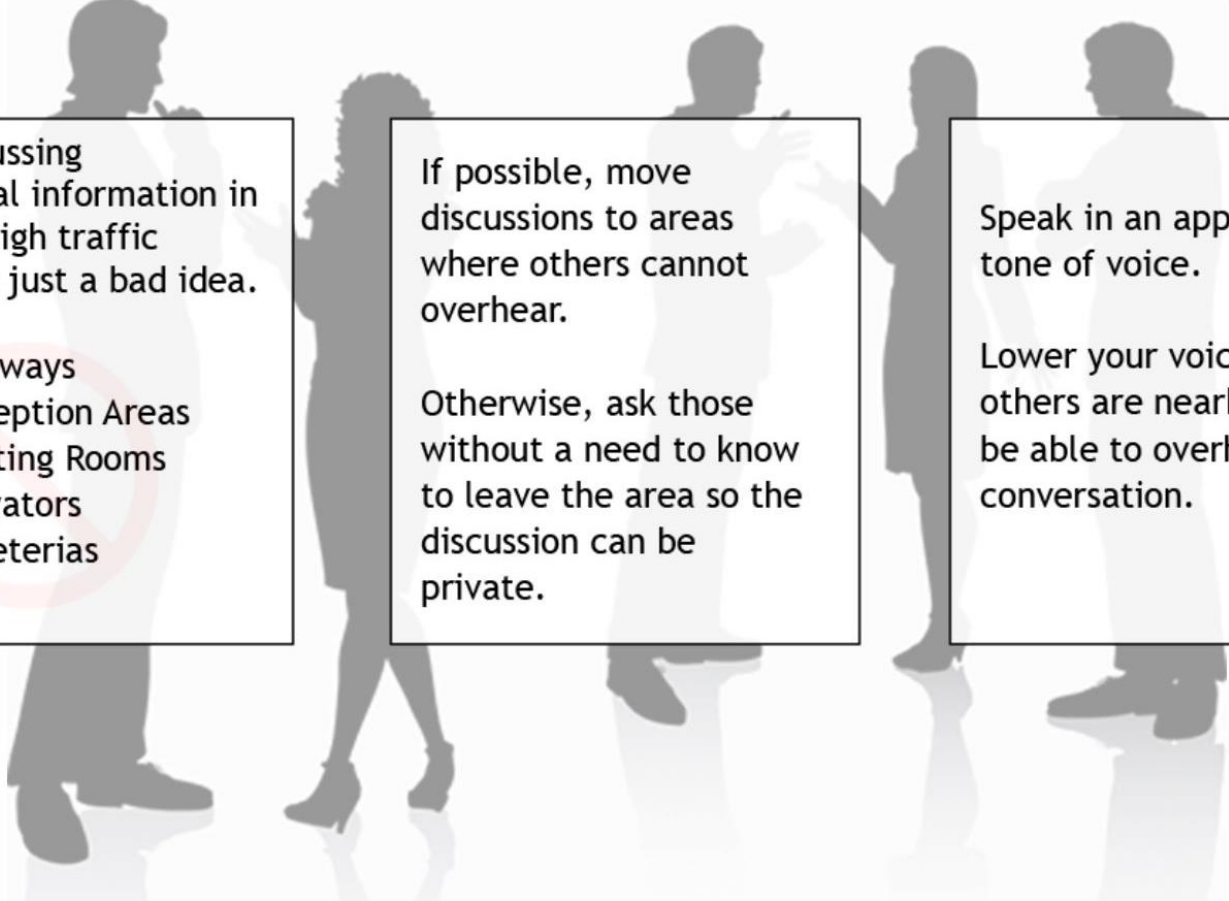
-  Yourself
-  Family Members
-  Children
-  Friends
-  Co-workers
-  Someone in the media



Be Aware and Keep Confidential Information Safe

- Turn computer monitors away from view of the public.
- Always lock or logout before stepping away from a computer.
- Documents with confidential information should be face down, covered, or in a folder if within sight of others.
- Scan hospital, clinic, or procedure rooms regularly and after each patient visit for documents left behind.
- In hospital, clinic, or procedure rooms, be sure that a patient is not able to see someone else's information on the monitor.
- When copying, printing, or faxing confidential information, do not leave the copier until job is complete, and ensure that nothing is left behind on the output tray.

Protecting Patient Privacy -- Verbal Communication



Avoid discussing confidential information in public or high traffic areas. It is just a bad idea.

- Hallways
- Reception Areas
- Waiting Rooms
- Elevators
- Cafeterias

If possible, move discussions to areas where others cannot overhear.

Otherwise, ask those without a need to know to leave the area so the discussion can be private.

Speak in an appropriate tone of voice.

Lower your voice when others are nearby and may be able to overhear your conversation.

Protecting Patient Privacy

Preventing Paper Privacy Problems

In 2016, there were several reported incidents at Virginia Mason Memorial that were related to papers containing PHI.

With that in mind . . .

- Consider whether it really needs to be printed.
- When handling documents, always verify each page corresponds to the patient you are helping.
- If you handle patient information in paper form, be sure to empty it into a secure Information Management locked shred bin. Daily disposal is considered best practice.



Reporting a Potential Breach

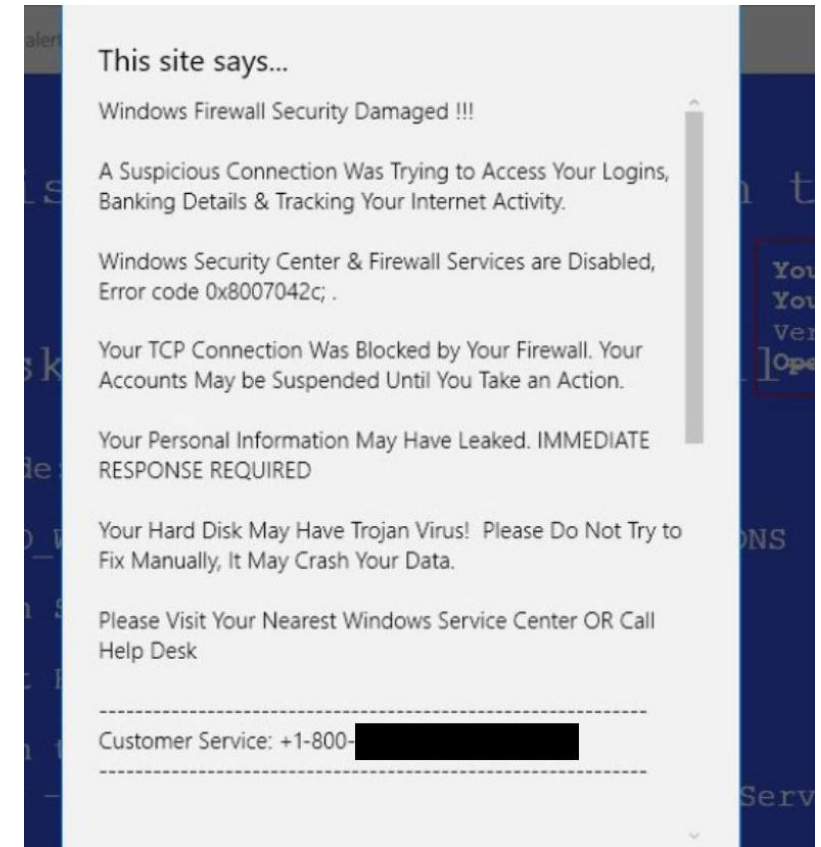
- You are **required** to report a potential breach to one of the following:
 - Department supervisor
 - YVM Integrity Hotline: (877) 684-8658
 - Privacy Office: privacyoffice@yvmh.org or (509) 225-2006
- If you have questions as to whether or not you should release information to someone, contact Health Information Management at (509) 577-5059
- If you have a privacy related question, please call the Privacy and Compliance Officer at (509) 574-7824 or (509) 574-7823

Internet Usage

- Yakima Valley Memorial's internet connection is for business use only.
- Please limit personal use of YVM's internet connection for web browsing, personal emails, messaging, etc.
 - These activities increase the risk of exposure to malware, viruses, and hackers.

Keep Our Systems Safe and Secure

- Examine search results carefully and avoid ads
 - Google has experienced issues with malicious ads displaying in search results.
- Type web addresses very carefully
 - Mistyping the address of a site (particularly a popular one) will often result in being taken to a malicious site. Hackers purchase web addresses that are common misspellings of popular sites.
- Never call anyone but YVM's Help Desk for support.
 - If you come across a page like this, do **NOT** call the number, click a bottom for live chat, complete a form, etc.
 - For support you should [only](#) contact the YVM Help Desk at (509) 875-8175



Cloud Services Must Be Approved by Information Services

T

Only Information Systems reviewed and approved cloud services are authorized to be used for **any** business purpose.

Signing up for a cloud service (e.g dropbox) without review/approval from Information Systems could place our systems at risk.

Legal Services needs to review any terms and conditions or contracts as well. Otherwise, Virginia Mason Memorial could be entered into a restrictive business agreement.

service
Terms

Virginia Mason
Memorial

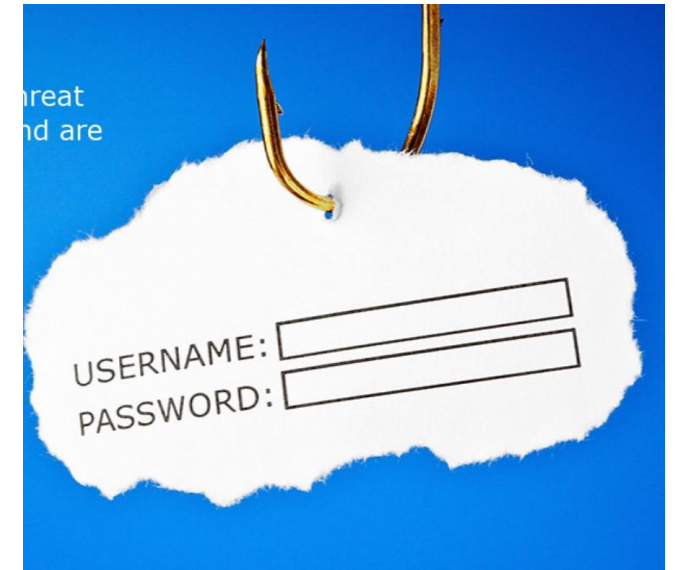
Social Media Guidelines

- The Social Media guidelines apply if you are posting about Yakima Valley Memorial in **any way**, from **any device**, from **any location**.
 - You must not post confidential or identifying information on social media.
 - It doesn't matter whether the intentions are good
 - It doesn't matter if the patient (or someone else) gives you permission.
- Team members and students must not take/post pictures or videos of activities at YVM.
- Before posting about YVM and/or your state of mind at work, consider how it might be perceived.
 - Ask yourself: "What would a patient think?"
 - Ask yourself: "What would my leaders or fellow students think?"
 - **If there is any uncertainty in your mind about whether you should post something, then you should not post it.**



Email Security – Phishing Attacks

- Phishing is a scam by which an email user is duped into revealing personal or confidential information, which the phisher can use to attack the individual or organization.
- It is not easy to obtain access to a system by hacking its security features. It is much easier to trick people into giving them the keys to the system through phishing.
- Healthcare institutions/workers are prime targets.
- To avoid being the next victim of a phishing attack, all of us must stop and think before we click/connect.



Identifying Phishing Attacks

- Watch out for strong emotions
 - Greed: emails that offer a reward of some kind if you click a link or enter your login information
 - Urgency: email provides a strict deadline for doing something
 - Curiosity: emails that promise to show you something exciting or forbidding
 - Fear: emails that threaten punishment or consequences
- Watch out for similar addresses. Phishers fool people with addresses that look similar to an organizations name.
 - Examples: yakimamemorial.org (real address) vs. yakimamemorial.my-mem.org (phisher's address)
 - Wellpoint.com (real address) vs. wel1point.com (phisher's address)

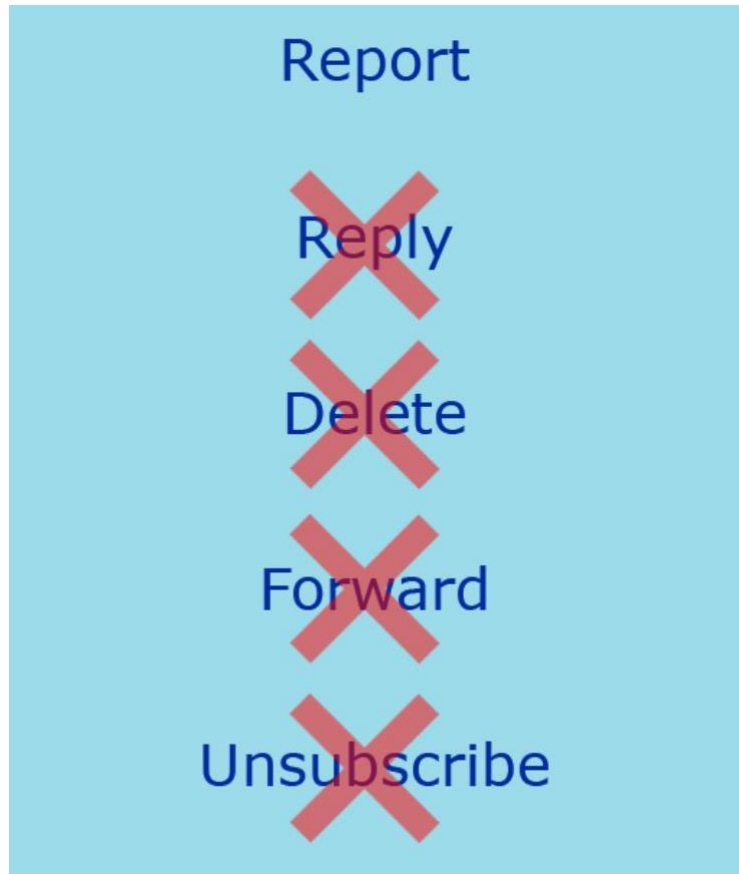


Identifying Phishing Attacks

- Email address: Be wary of email addresses with incorrect spellings, or a company email coming from a personal account. Also look at the To: and CC: fields to see if the email is being sent to people you don't know or work with.
- Generic greetings: Be wary of generic greetings. A trusted organization that you are doing business with should know your name. Also ask, am I expecting an email from this company?
- Grammar/spelling errors: Be suspicious of emails with spelling or grammar mistakes.
- Email links: Be very careful with links provided in emails. **In most cases, we recommend not clicking email links at all.** If you must click a link, be sure to hover over the link to see its destination first. If the address do not match, it is most likely a phishing email.
- Attachments: Be wary of attachments. Only open those you are expecting.



Please Report Any Possible Threats

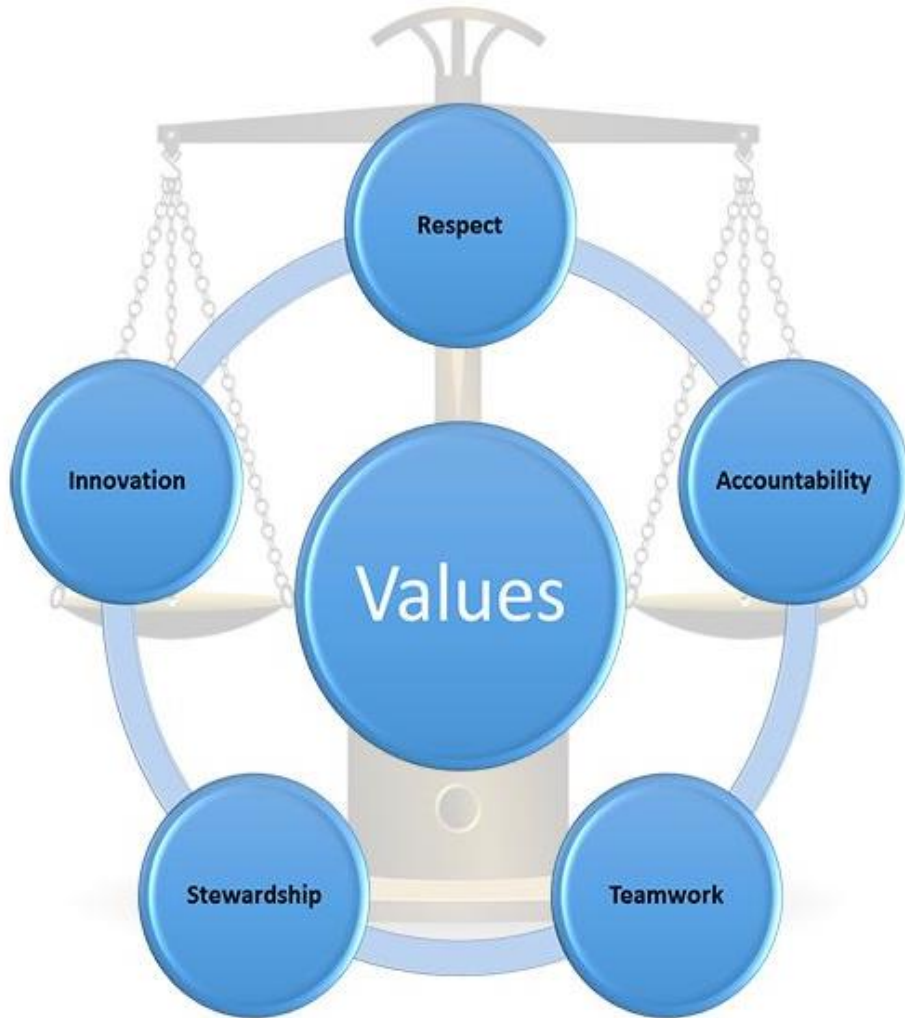


If you receive a phishy email, or if an email directed you to a webpage that is suspicious, contact the I.S. Help Desk at (509)575-8175

You may be the first to report a new threat, and [quick reporting may help Virginia Mason Memorial to thwart an attack!](#)

Do not be afraid to report it. Also, please do not reply, forward or delete the email.

Integrity Program



- Yakima Valley Memorial honors integrity, accountability, honesty and ethical behavior as a fundamental value.
- Each team member, including students, must perform their duties in accordance with these values
- All team members are charged with the responsibility to know the legal standards which relate to their duties and to follow them accordingly
- The Integrity Program demonstrates our commitment to comply with our Standards of Conduct, laws, regulations, and policies/procedures

The Integrity Program Supports You



- We assist with interpretation of law, policies and procedures.
- Our program empowers all team members to prevent, detect and resolve any issue.
- Our open lines of communication support our team members to speak up and hold each other to the highest standards.
- We investigate and manage all issues through the resolution process.

Integrity Program Hotline:

1-877-684-8658



Standards of Conduct

Yakima Valley Memorial strives to be the quality leader and fulfill our mission to improve the health and well-being of the patients we serve through our values of integrity, teamwork, respect, excellence, stewardship and service.

We are committed to preserving the trust and respect of those we serve. The values in the Standards of Conduct extend beyond our obligation to conduct our business in accordance with all applicable standards and laws.

****Please see Appendix for complete Standards of Conduct*



Standards of Conduct

The Standards of Conduct provide general guidance for our conduct. It does not address every situation where the exercise of integrity, honesty or ethical decision-making may be necessary.

In some instances, more explicit guidance can be found in YVM policy, procedure, or process.



Violations of the Standards or any policies or procedures will result in disciplinary action, up to and including termination of employment or privileges when warranted.

Important Contact Information

Kim Wakeman, Student Experience Specialist:

- (509) 249-5670
- KimberlyWakeman@yvmh.org

Employee Health:

- (509) 574-5830

Information Systems Help Desk:

- (509) 575-8175

Security:

- (509) 494-7233 or ext. 7233 (SAFE)



APPENDIX

- Standards of Conduct
- Workforce Privacy and Security Training Policy
- HIPAA Privacy Guidelines
- Social Media Guidelines
- Acceptable Use

STANDARDS OF CONDUCT POLICY

Yakima Valley Memorial

Yakima Valley Memorial ("YVM", "Memorial") strives to be the quality leader and fulfill our mission to improve the health and well-being of the patients we serve through our values of integrity, teamwork, respect, excellence, stewardship and service. We are committed to preserve the trust and respect of those we serve. The values in the Standards of Conduct ("Code") extend beyond our obligation to conduct our business in accordance with all applicable standards and laws.

These Standards provide general guidance for our conduct. It does not address every situation where the exercise of integrity, honesty or ethical decision-making may be necessary. In some instances, more explicit guidance can be found in YVM policy, procedure, or process. However, these Standards will be the guide conduct where explicit policy does not exist or an existing policy would appear to conflict with the Standards. Violations of the Standards or any policies or procedures will result in disciplinary action, up to and including termination of employment or privileges when warranted.

The Yakima Valley Memorial Board of Directors has adopted these Standards of Conduct and instituted the Integrity Programs to clearly state the principles and standards of conduct necessary to demonstrate our commitment to our values, and to ensure compliance with laws that govern YVM activities.

Memorial's reputation has been built, and ultimately depends on individual integrity and collective actions of our workforce. These Standards of Conduct apply to Yakima Valley Memorial and its affiliates (including but not limited to Memorial Physicians, PLLC, Central Washington Healthcare Partners, LLC dba Signal Health, The Memorial Foundation and others).

These Standards govern the actions of all workforce members, including Board members, corporate officers, staff, medical staff, independent contractors, volunteers, students, and others working on Yakima Valley Memorial property or associated with Yakima Valley Memorial. Each workforce member is expected to read, understand and comply with the Code and request clarification when necessary.

Standards of Conduct

Through adherence to these Standards, our workforce members should make sound ethical decisions during their day to day activities. These Standards do not substitute for common sense, individual judgment, and personal integrity, for which we are all accountable. However, these are common standards for our actions and attitudes. We must adhere to these standards to fulfill our mission, vision, and values.

Focus on Patients

We will provide exceptional quality care to our patients.

We will treat our patients, visitors, and all other workforce members with dignity, courtesy and respect with our spoken and unspoken behavior, regardless of race, nationality, age, religion, creed, the presence of a physical, mental or sensory disability or perceived disability, gender, sexual orientation, marital status, union status, veterans status, financial ability or any other basis prohibited by local, state or federal laws.

We will avoid any inappropriate and disruptive behaviors that may interfere with patient care delivery and services or any acts that interfere with the orderly conduct of the organization's or individual's abilities to perform their jobs effectively. Disruptive and inappropriate behavior includes, but is not limited to, abusive language, condescending voice intonation, angry outbursts, bigotry, bullying, demeaning behavior, offensive jokes, physical violence, and sexual misconduct.

We will employ safe practices and maintain a safe environment for our patients, visitors and workforce. We will utilize our Safety programs to identify potentially unsafe environments, practices, or patient care.

We will maintain a workforce free of any unauthorized substances or alcohol while on property.

We will respect patients' privacy rights by maintaining patient information in accordance with all laws and policies.

We will ensure the integrity of research and the appropriate protection of human subjects.



Focus on Staff

We will embrace open, honest, fair, and respectful communication.

We will promote the reputation of the Health System with our honesty and integrity by not making false or misleading oral or written statements during the performance of our duties.

Focus on Corporate Responsibility

We will operate in accordance with all applicable laws, regulations and standards.

We will conduct our duties for the benefit and interest of the Health System and avoid conflicts and any appearance that our responsibility to the Health System might be compromised by outside obligations or interests.

We will take every reasonable precaution to ensure that our medical service documentation, coding and billing is accurate, timely and in compliance with our policies and with laws and applicable standards governing these complex processes.

We will prepare and maintain financial reports, accounting records, and all other business and patient care records accurately and completely, and in accordance with applicable standards.

We will avoid offering or accepting inappropriate gifts or other things of value to or from our patients or vendors.

We will provide equal opportunity in all aspects of employment and will not tolerate discrimination or harassment of any kind. Derogatory comments, unwelcome sexual advances and similar behavior are prohibited.

We will support appropriate boundaries between our team members and between our team members and our patients to ensure our focus on integrity.

We will be responsible to question, challenge and report any situations that potentially violate these Standards, a Health System policy, or applicable law, without fear of retribution, intimidation, or retaliation.

We will protect and safeguard the Health System's funds, assets, confidential, and/or proprietary information and Health System information related to our vendor relationships.

We will market Health System services honestly and fairly.

We will cooperate with legally authorized government investigations, including Health System leadership, Legal Services and the Compliance Officer as soon as we are aware of the investigation. We will not destroy or alter any documents or records in anticipation of a request by a government agency or court, we will not destroy or alter any documents or records in anticipation of a request by a government agency or court, we will not make false or misleading statements to a government official, and we will not attempt to influence others as the investigation progresses.

Reporting

We all are responsible for ensuring compliance with these Standards. This responsibility includes an obligation to seek answers to questions regarding these Standards, policy, or law, and an obligation to report a potential violation of these Standards, policy or law. In either of these instances, our workforce members should contact their supervisor, another leader, the Compliance Officer, Integrity Program, or the Legal Services Department.

Additionally, Yakima Valley Memorial has a secure and confidential Integrity Help Line at **1-877-684-8658** that may be used for inquiry or for reporting potential Standards violations.

All inquiries and reports made to the Integrity Program will be thoroughly investigated and if necessary, appropriate action taken to resolve the issue.

A supervisor or manager to whom a report of a suspected violation is made is obligated to pursue resolution and involve the appropriate administrators and the Integrity Program.

The Health System is committed to protecting those who, in good faith, report actions that they believe are violations to these Standards, Health System policy, or applicable laws. We will not engage in retaliation or reprisal against anyone who properly reports violations of law, regulation or policy. Anyone who feels that retaliation has occurred subsequent to a report of non-compliance should immediately notify Human Resources, the Compliance Officer, Integrity Program, or Legal Services Department.

Integrity Standards in Action (ALL NEW SECTION)

The Health System commits to supporting each workforce member in understanding their role in the integrity process: doing the right thing-- the first time, and every time. When we have not done the right thing, we must correct our mistake, and when we don't know what we should do, we must ask for help.



The Standards of Conduct support the workforce to conduct business using sound ethical practices, and the healthcare industry is highly regulated and complex rules and regulations exist at the federal and state level which govern the Health System. The following address some complex, integrity-related topics which are important to the healthcare industry:

Preventing and Detecting Fraud, Waste and Abuse

The Health System will investigate allegations of fraud, waste or abuse and, where appropriate, take corrective action, including, but not limited to civil or criminal action. A number of federal and state laws are designed to prevent and detect fraud, waste and abuse in government health care programs and impose liability on any person or entity that submits a claim to the federal government that is known (or should have known) to be false. The federal False Claims Act (FCA) and similar state laws prohibit the knowing submission of a false claim to the government for reimbursement, and violations of the FCA can result in significant civil penalties and damages, an obligation to enter into a Corporate Integrity Agreement with the government, exclusion from federal healthcare programs, or even criminal prosecution.

The FCA allows private parties to bring suit on behalf on the government against parties alleged to have committed fraud, protecting these “whistleblowers” from retaliation. Both the federal False Claims Act and state law provide protections against employer retaliation of an employee who reports fraud to the government.

For detailed information on the Federal False Claims Act, please refer to:

Federal False Claims Act (31 U.S.C §§ 3729-3733) http://justice.gov/civil/docs_forms/C-FRAUDS_FCA_Primer.pdf

For detailed information on the Washington False Claims Act, please refer to: ***Washington Medicaid False Claims Act (RCW 74.09) <http://apps.leg.wa.gov/rcw/default.aspx?cite=74.09>***

Anti-Kickback Statutes

In general, anti-kickback laws prohibit the offering, payment, solicitation or acceptance of any form of payment for the referral of a patient. Health care professionals and entities are prohibited from paying directly or indirectly for referrals. Referrals can refer to hospital admissions, durable medical equipment, ordering a particular lab test or drug, or another type of healthcare activity. Payment is defined as any type of cash payment or promise of payment or payment in kind.

Stark Laws

These laws prohibit physicians and their immediate family members from making referrals for certain designated health services payable to Medicare to an entity with which they have a financial relationship (ownership, investment or compensation), unless a specific exception applies. The Laws also prohibit the entity from presenting claims to Medicare for those referred services. Any questions related to this topic should be directed to the Compliance Officer.

Conflicts of Interest

A conflict of interest may exist if a workforce member’s outside activities or personal interests influence or appear to influence the workforce member’s ability to make objective decisions in the course of carrying out responsibilities and obligations to the Health System. Conflicts must be disclosed and resolved so all parties involved understand the concerns involved, and those not involved in the conflict can make the appropriate business decision.

Emergency Medical Treatment and Active Labor Act (EMTALA)

Patient’s emergent medical care will not be delayed by financial screening in accordance with EMTALA. The Federal government has enacted the EMTALA (anti-dumping”) law to ensure that patients receive a medical screening examination and are not transferred from one emergency room to another facility unless it is medically appropriate.

Safe Environment

We are committed to protecting and enhancing the environment in which we serve our community. A safe environment supports physical safety and security, and mitigates or prevents contact with hazards without appropriate protections. Reducing the impact of a healthcare organization on the environment through sustainability efforts also supports a safe environment by reducing wastes and preserving natural resources.

Drug Free Workplace

We support a drug free environment.



Workforce Privacy and Security Training Policy

PURPOSE: The purpose of this policy is to ensure that Yakima Valley Memorial's Workforce (defined below to include both Yakima Valley Memorial and Memorial Physicians Workforce members) has the training necessary to protect the privacy and security of Protected Health Information. Yakima Valley Memorial is committed to ensuring that its Workforce is trained in policies and procedures that protect health information from misuse and unauthorized disclosure. Additionally, federal law requires that Workforce members receive training in privacy and security policies and procedures.

SCOPE: All Employees and other Workforce members.

All Workforce members who are onsite at Yakima Valley Memorial (defined below to include Yakima Valley Memorial and Memorial Physicians), or who may otherwise access and use Yakima Valley Memorial systems containing Protected Health information. This policy also applies to on-site service providers who may access, use or disclose PHI.

POLICY:

Yakima Valley Memorial provides training in relevant privacy and security policies and procedures, to its Workforce who are onsite at Yakima Valley Memorial or who may otherwise access and use Virginia Mason Memorial systems containing Protected Health Information. **Workforce includes:**

Staff: Employees of Yakima Valley Memorial, to whom a Yakima Valley Memorial entity issues IRS Forms W-2, including employed professional staff; and

Non-staff: Individuals working on behalf of Yakima Valley Memorial who are not employees, including:

- Community Provider
- Contractor – On-Site, examples include ABM, Crothall, ARAMARK
- Health Care Workers
- Independent Contractor
- Job Shadows
- Students
- Temporary Agency Staff — Clerical and Health Care Professionals
- Vendor Staff– Sales and Service
- Volunteer

All new Workforce members shall complete the Privacy and Security Training as a requirement of hire or initial assignment, within timeframes established by Yakima Valley Memorial. Thereafter, annual Privacy and Security Training will be assigned as part of Yakima Valley Memorial's Annual Training requirements consistent with the schedule and requirements determined by Yakima Valley Memorial.

The Privacy Officer provides Privacy and Security Training updates to the privacy and security Learning Management System modules, as needed. The Privacy officer as warranted and at the Privacy Officer's discretion, will provide in person Privacy and Security Training for new Workforce members, or in person "refresher" Privacy and Security Training.

All Workforce members "sign" a Learning Management System agreement entitled "Confidentiality, Privacy and Security Agreement" which appears after completion of the Privacy and Security Training modules on the Learning Management System. A form of the "Confidentiality, Privacy and Security Agreement" is attached as Exhibit A.

The Learning Management System tracks and maintains records of all Workforce members who have successfully completed the required privacy and security training modules and "signed" the Confidentiality, Privacy and Security Agreement, in compliance with this policy. Such documentation shall be retained six (6) years



All efforts will be made for Workforce members to use the online Learning Management System to meet the requirements of this policy. However, to the extent that there remain Workforce members who cannot access the Learning Management System, print copies of the modules will be provided to them by department managers, for purposes of completing the Privacy and Security Training. Such Workforce members sign the paper copy of the Confidentiality, Privacy and Security Agreement. Documentation of Privacy and Security Training, including signed copies of the agreement, are retained by the accountable manager for that Workforce member.

Department managers are responsible for ensuring Workforce member completion of the Learning Management System Privacy and Security Training modules and the Confidentiality, Privacy and Security Agreement.

Yakima Valley Memorial staff (employees) who violate this policy are subject to Yakima Valley Memorial's progressive discipline policy. Non-staff members who violate this policy are subject to limitation and/or termination of their affiliation, as determined by Yakima Valley Memorial.

DEFINITIONS:

Community Provider: An individual physician, allied health professional and other credentialed provider practicing at, but not employed by Yakima Valley Memorial.

Contractors (On-Site): Workers who work for an independent vendor or company but are assigned to Virginia Mason Memorial and work on-site. Contractors include, but are not limited to, ABM, Crothall, ARAMARK.

Health Care Worker: A non-credentialed individual who furnishes health care or social services on Yakima Valley Memorial property.

HIPAA: Health Insurance Portability and Accountability Act of 1996, and its implementing regulations.

Independent Contractors: Self-employed individuals who are retained by Yakima Valley Memorial on a contract or project basis to perform specific tasks or services. They are usually compensated on a contract or fee for service basis.

Yakima Valley Memorial's Learning Management System: Learning Management systems include, but are not limited to, Simplyr, VSys one, Healthstream.

Job Shadows: An individual who, under the supervision of a Yakima Valley Memorial employee, observes but does not participate in an activity.

Non-staff: Individuals working on behalf of Yakima Valley Memorial who are not employees, including:

- Community Provider
- Contractor – On-Site, examples include ABM, Crothall, ARAMARK
- Health Care Workers
- Independent Contractor
- Job Shadows
- Students
- Temporary Agency Staff — Clerical and Health Care Professionals
- Vendor Staff– Sales and Service
- Volunteer



Privacy Officer: The privacy official who is responsible for the development and implementation of the Yakima Valley Memorial policies and procedures with respect to HIPAA compliance. Also the designated privacy contact or office responsible for receiving complaints with respect to HIPAA privacy compliance and who is able to provide further information about matters covered by the Notice of Privacy Practices (NPP) required by HIPAA.

Privacy and Security Training: Privacy and security training required by law and Yakima Valley Memorial policy. Methods of training may include in person; online, or paper based, as determined by Yakima Valley Memorial.

Protected Health Information or PHI: is any information, including demographic information that has the potential of tying the identity of the patient to their health record. Applies to information transmitted or maintained in any form or medium, including electronic, paper, and oral. It is the subset of individually identifiable health information to which the privacy protections of HIPAA apply. (This term does not include educational records governed by FERPA, and employment records.)

Staff: Employees of Yakima Valley Memorial to whom a Yakima Valley Memorial entity issues IRS Forms W-2, including employed professional staff; and

Student: An individual who is receiving academic credit through an affiliation agreement with a defined educational program.

Temporary Agency Staff: Individuals provided by a temporary staffing agency to provide a replacement for an employee who is away from work for vacation, leave of absence, or illness. A temporary employee may be short or long-term.

Vendor: A manufacturer, distributor or service provider from which Yakima Valley Memorial purchases goods and/or services.

Yakima Valley Memoria: Collectively, Yakima Valley Memorial Hospital Association and Memorial Physicians PLLC.

Volunteer: A person who performs authorized services to Yakima Valley Memorial without compensation.

“Workforce” or “Yakima Valley Memoria Workforce:” All individuals working on behalf of Yakima Valley Memoria, including staff and non-staff.

REFERENCES:

HIPAA Privacy Rule 45 CFR Part 164.530(b) and (e) HIPAA Security Rule 45 CFR Part 142.308(a) (12) Washington Uniform Health Care Information Act

KEYWORD Indexes:

Privacy, Security, Workforce Training

Effective Date September 21, 2017



HIPAA Privacy Guidelines (“Guidelines”)

These guidelines are to ensure all Workforce Members protect the confidentiality and integrity of Protected Health Information (PHI) and Individually Identifiable Information (III), which has been entrusted to the organization for use and safekeeping. Yakima Valley Memorial has both ethical and legal obligations to recognize that patients, employees and donors have a right of privacy and to respect those rights. All Yakima Valley Memorial workforce must abide by the following set forth guidelines:

Protect the Privacy and Security of PHI and III by accessing and using only the information necessary to perform job related duties.

Act as a responsible information steward and treat all health information, financial, demographic, and lifestyle information as confidential and will provide patients with current Notices of Privacy Practices, not disclose PHI or III unless the patient or their authorized personal representative has properly authorized the release or the release is permitted or authorized by law, or report any concerns related to privacy of PHI or III to their immediate supervisor, the Integrity Hotline, the Chief Information Security & Privacy Officer, or Legal Services.

Investigate patient and Workforce Member concerns or complaints of potential breaches of Privacy and Security.

Not access the PHI or III of friends or family members, including minor children. A patient may submit written authorization to allow an individual to obtain a copy of their medical record through the Release of Information process or be granted access to their information as publically offered by VMM via the Patient Portal.

Not access their own PHI unless granted access to their information via the Patient Portal. A Workforce member may obtain a copy of their medical record through the Release of Information process.

Obtain valid authorization prior to releasing PHI to sectors such as law enforcement and government.

The Privacy Office will perform routine auditing of accesses made to the electronic medical record, including regular review records of audit logs, access reports, and incident tracking reports. The Privacy Office may perform these audits as part of a routine plan, following patient or Workforce Member complaint, based on the status of a patient (i.e. family member, media coverage, co-worker or VIP), or other circumstances. Any questionable accesses will be further investigated. YVM Workforce Members and Business Associates are required to cooperate with an investigation.

To remain in compliance, Yakima Valley Memorial suggests that you review the Policy, as well as the other website policies, at regular intervals. By continuing to post any content after such new terms are posted, you accept and agree to any and all such modifications to these guidelines.

about what is appropriate to include in your social media profile(s).



Social Media Sites Guidelines (“Guidelines”)

The following are guidelines for Yakima Valley Memorial (“YVM”, “Memorial”) team members who participate in social media. Social media includes personal blogs and other websites, including Facebook, Twitter, YouTube, Instagram, LinkedIn and many others. These guidelines apply whether team members are posting to their own sites, commenting on other sites or providing information that others may post on their social media channels:

- Follow all applicable YVM policies. These include policies pertaining to patient confidentiality; computer, email and Internet use; photography and video; and release of patient information to media.
- You must not share confidential or proprietary information about YVM, and you must maintain patient privacy at all times.
- Taking video and pictures of any activity at YVM and posting them on social media channels, websites, discussion forums or sending them to anyone – whether it’s a patient, team member, medical colleague, friend or family member – is prohibited. Team members are also prohibited from posting YVM’s logo on social media sites. * YVM’s Acceptable Use Policy addresses social media and includes expectations for team members who choose to participate (see page 4 of policy).
- Write in the first person. Where your connection to YVM is apparent, make it clear that you are speaking for yourself and not on behalf of YVM. In those circumstances, you should include this disclaimer: “The views expressed on this [blog; website] are my own and do not reflect the views of my employer.” Consider adding this language in an “About me” section of your blog or social media profile.
- If you identify your affiliation to YVM, your social media activities should be consistent with YVM’s high standards of professional conduct.
- If you communicate in the public internet about YVM or YVM-related matters, you must disclose your connection with YVM and your role with the organization.
- Be professional, use good judgment and be accurate and honest in your communications; errors, omissions or unprofessional language or behavior reflect poorly on YVM, and may result in liability for you or the organization. Be respectful and professional to fellow team members, business partners, competitors and patients.
- Ensure that your social media activity does not interfere with your work commitments.
- YVM strongly discourages “friending” of patients on social media websites. Team members in patient care roles generally should not initiate or accept friend requests except in unusual circumstances, such as the situation where an in-person friendship pre-dates the treatment relationship.
- YVM discourages team members in management/supervisory roles from initiating “friend” requests with team members they manage. Managers/supervisors may accept friend requests if initiated by the team member, and if the manager/supervisor does not believe it will negatively impact the work relationship.
- YVM does not endorse people, products, services and organizations. On social media websites such as LinkedIn, where your affiliation to YVM is known, personal recommendations should not be given or requested.
- Unless approved by YVM Communications, your social media name, handle and URL should not include YVM’s name or logo.
- Ask YVM Communications (509) 249-5221, if you have any questions about what is appropriate to include in your social media profile(s).



ACCEPTABLE USE-INFORMATION SECURITY

Yakima Valley Memorial (YVM) is responsible for securing its computer systems, associated data, and telecommunications network. In addition, YVM and affiliated agency employees are responsible for preventing the occurrence of inappropriate, unethical or unlawful use of such systems and policies.

Access to computer systems and networks owned or operated by YVM imposes certain responsibilities and obligations and is granted subject to Hospital policies, and local, state, and federal laws. Acceptable use is always ethical, legal, maintains patient confidentiality, protects the organizations interests, and shows restraint in the consumption of shared system resources.

YVM takes protection of our patients' Protected Health Information (PHI) very seriously. In order to protect our patients and employees privacy, please use the following best practices:

Access patient records only as needed for your job duties.

If someone you know is receiving care in your area and you do not feel comfortable participating in their care, notify your supervisor of the relationship to the patient, discontinue care, and do not access that patient's records.

Do not access your own records—contact Health Information Management to request a copy of your records.

Share PHI only with Business Associates, other healthcare providers for continuum of care, or with other entities as required by law.

Store and transmit PHI only using applications or network locations designated for those purposes. If you have a use case not covered by the list, contact IS and work with them to find an appropriate solution.

Any employee picture uploaded to a Memorial applications must be professional.

For any questions please consult your manager, Information Systems or Privacy Officer

Acceptable Use

Acceptable use of information systems includes, but is not limited to:

Using computing resources only for authorized purposes.

Protecting your computer equipment, user-ID, and password from unauthorized use.

You are responsible for all activities associated with your user-ID or that originate from your credentials.

Accessing only files and data that are your own, which are publicly available, or to which you have been given authorized access.

Using only legal versions of copyrighted software in compliance with vendor license requirements and as approved by the YVM Information Systems department.

Unacceptable Use:

Unacceptable use of information systems includes, but is not limited to:

Using another person's user-ID or password.

Using another person's system, files, or data without permission.

Attempting to circumvent or subvert system or network security measures.

Engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.

Using YVM systems for commercial, political, or extensive personal use.

Installing or using illegal copies of copyrighted software, or any other software provided by the Information Systems department.

Using mail or messaging services to intimidate or otherwise harass another person.

Engaging in any other activity that does not comply with the general principles presented above.

No data shall be shared with any entity who is not on the MFOS Business Associates Agreement list unless required by law.

To verify BAA status for a vendor contact the MFOS Chief Information Officer.



ACCEPTABLE USE-INFORMATION SECURITY

Shared Admin Credentials for System Builds/Implementation (IS Department Only):

After a system has gone live, all shared admin credentials must be deactivated and new credentials per user must be assigned for security purposes

ENFORCEMENT.

Abuse of YVM information systems can compromise the security and privacy of patient information and expose employees and YVM to legal risks. YVM considers any violation of acceptable use principles and guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on Hospital systems. Violators will be subject to appropriate disciplinary action as prescribed in other Hospital policies.

All activity will be monitored, logged and is available for review if a user's activity is in question.

IS may use technical means to enforce compliance, including antivirus software, Web filtering, enforced configuration of certain workstation configurations, routine scans for PHI in inappropriate locations, disabling removable media, and other methods to ensure the security and proper operation of YVM systems and data.

WORKSTATION USE & SECURITY

Workstations are available to authorized YVM and Affiliates workforce members to access the applications that constitute the Information System of the organization. These workstations must be used appropriately as addressed above in the acceptable use section and must be protected from unauthorized access.

Report lost or stolen Memorial devices to Information Systems Help Desk.

Definitions:

Workforce means employees, volunteers, trainees, and other persons who perform work on behalf of YVM and are under the control of the organization, whether or not they are paid.

Workstation means an electronic computing device, for example, a laptop, tablet, smartphone or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment (provided by YVM or personally owned).

PROCEDURE

Workstation Usage:

Workstations should be used for YVM business only. Nothing in this section prohibits use of email during nonworking time to discuss terms and conditions of employment with coworkers.

Antivirus Software:

Antivirus software is installed by YVM Information Systems department. Do not try to disable it or interfere with its operation.

Unattended workstations:

Workforce members must log-off or password lock their workstations when they will be leaving the workstation unattended. All users are liable (individual or organization?) and responsible for all activity performed with their credentials.

MOBILE DEVICES

Because mobile devices are easily lost, stolen, or otherwise compromised, it is not appropriate to store or transmit PHI using mobile devices.



ACCEPTABLE USE-INFORMATION SECURITY

Users of mobile devices (laptops, tablets, cellphones, etc.) which contain confidential or sensitive information must protect the device and the information from loss, damage or unauthorized access. When unattended in a controlled environment, the device should be inaccessible through the use of physical locks or software, which prevents others from accessing the information on the device. Mobile devices should never be left unattended in an uncontrolled environment, such as public hallways, cafeteria, waiting rooms, etc. Configuring your mobile device to access YVM email also enables a “remote wipe” feature, which allows IS to force the device to erase itself to protect any private information that may have been stored on the device. Notify IS immediately if your mobile device is lost, stolen, or otherwise compromised.

The use of personal cell phones for the collection and transmission of unsecured PHI (including photos) is prohibited. Violators will be subject to appropriate disciplinary action as prescribed in other YVM policies. This policy applies to both YVM-owned and personally-owned device. Users are liable for any breach or loss of PHI.

INTERNET USE

The Internet, like all hospital resources, is to be used for professional purposes. In addition, specific policies and procedures are in place to protect and preserve hospital resources. The Information Systems department is the sole administrator and technical manager of all hospital Internet resources. Different policies and procedures exist dependent upon the type of Internet access (modem or network). Individual employees must adhere to the following Internet acceptable use policy at all times.

Acceptable Use

Acceptable use of YVM Internet resources includes, but is not limited to:

- Using Internet browsing for authorized and appropriate purposes only.
- Protecting your login and password from unauthorized use.
- Accessing only websites that relate to your position at YVM.
- PHI only exchanged with businesses for continuum of care or with BAA established through secure method.

Unacceptable Use:

Unacceptable use of YVM Internet resources includes, but is not limited to:

- Unauthorized file download. If file downloads are authorized, copyright laws are not to be violated by downloading unauthorized software over the Internet.
- Unauthorized or inappropriate web browsing.
- Interference with Information Systems’ efforts to manage or maintain a secure and functional Internet environment.
- Sharing of PHI via email, social media, group forums or any other form of unauthorized disclosure.

TEXT MESSAGING

Text messaging of PHI is prohibited unless through approved software provided by and supported by the MFOS Information Systems department. For a list of approved text messaging software applications please see the acceptable use policy.

SOCIAL MEDIA

The use of social media on YVM equipment and time is prohibited unless specified in the users’ job description and role.

Disclosure of PHI is prohibited and will result in appropriate disciplinary action as prescribed in other YVM policies.



ACCEPTABLE USE-INFORMATION SECURITY

EMAIL

Acceptable use of the YVM email system is always ethical, legal, maintains patient and employee confidentiality, protects the organization's interests, enhances communication in support of business needs, and shows restraint in the use of shared computer system resources.

YVM email is primarily a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the following legal risks of email:

If you send emails with any violent, demeaning, abusive, offensive, racist, or obscene remarks, you and YVM can be held liable.

Never send any unsecured PHI through the email.

If you send unsecure confidential information or PHI, you and YVM can be held liable.

If you unlawfully forward or copy messages without permission, you and YVM can be held liable for copyright infringement.

If you knowingly send an attachment that contains a virus, you and YVM can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this policy, the user will be fully liable and YVM will disassociate itself from the user as far as legally possible.

The following rules are required by law and are to be strictly adhered to:

Do not forge or attempt to forge email messages.

Do not send email messages using another person's email account.

Do not disguise or attempt to disguise your identity when sending mail.

Do not break into, or attempt to gain unauthorized access to, the YVM or any other organization's email system(s).

Do not undertake deliberate activities that waste staff effort or networked resources.

Do not deliberately introduce any form of computer virus or malware into the YVM corporate network

Nothing in this section prohibits use of email during nonworking time to discuss terms and conditions of employment with coworkers.

System Monitoring:

You must have no expectation of privacy in anything you create, store, send or receive on the YVM company computer system. Your emails can be monitored and logged without prior notification to you if MFOS deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, YVM reserves the right to take disciplinary action, which could include termination and/or legal action.

Email Account Security:

All email accounts maintained on the YVM email system are property of YVM. Passwords should not be shared or given to other people and should be changed at least every 90 days as required by the Information Systems Department.

INSTANT MESSAGING

Instant messaging (IM) does not have adequate security controls for handling unencrypted PHI and should not be used to share or transmit PHI.



ACCEPTABLE USE-INFORMATION SECURITY

REMOVABLE STORAGE MEDIA DEVICES

Examples of removable storage media include CDs, DVDs, and USB drives (a.k.a. “thumb drives”).

These media are too easily lost or stolen to be trusted with unencrypted PHI. IS may vet and support certain media or applications for securing data before storing it on removable media. For recommendations on acceptable removable storage devices please consult IS.

CLOUD STORAGE

To process, store, or transmit PHI using cloud services is prohibited unless a current Business Associate Agreement with a service provider is established.





YAKIMA VALLEY
MEMORIAL