POLICY

Responsible Use of Systems and Electronic Communications

Category: Organizational
Sub-Category: Information management **Other:** Click here to enter text.
Type: POLICY
Status: Active
Last Reviewed: 06/11/2020
Regulatory Source(s): The Joint Commission **Other:** OCR
Regulatory Citation Number(s): 45 CFR Parts 160 – 164
Citation title: HIPAA Privacy Rule, HIPAA Security Rule
Foundational Mirrored Policy: Yes

PURPOSE:
Yakima Valley Memorial expects all individuals who use its systems and clectronic communications to do so in a responsible manner. The purpose of this policy is to set clear expectations for this use. Users and all others who use Yakima Valley Memorial systems and electronic communications are responsible to read and understand this policy in its entirety.

SCOPE: All Employees/Workforce

POLICY:
Yakima Valley Memorial prohibits use of its systems to violate Yakima Valley Memorial policies or the law.

GUIDING PRINCIPLES OF RESPONSIBLE USE

- Regulatory Compliance. Yakima Valley Memorial will safeguard information in a manner consistent with applicable requirements of federal, state and local law and regulations, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) and the Joint Commission Information Management standards.

- Common Sense and Good Judgment. No policy can adequately substitute for personal common sense and good judgment. At a minimum, users are expected to apply these attributes to their daily job-related activities and their electronic communications. Users are expected to follow Yakima Valley Memorial policies, including Yakima Valley Memorial's Standards of Conduct and follow Yakima Valley Memorial service standards for interacting with patients and coworkers.

- Respectful Treatment of Others. Be respectful and professional to fellow users, business partners, competitors and patients. Users may not use systems in any way that may be seen as malicious, obscene, threatening, disparaging to others, or that might constitute harassment or bullying.

- No Right of Privacy: Yakima Valley Memorial systems have been purchased and installed to facilitate business process and electronic communications. Although each user may have individual access rights, the systems are the property of Yakima Valley Memorial. Users should never assume electronic communications are private and confidential. Since personal messages can be accessed by Yakima Valley Memorial management without prior notice, staff should not

use Yakima Valley Memorial systems to transmit any messages they would not want accessed by a third party.

Yakima Valley Memorial reserves the right, in its discretion and without user permission, to review any Yakima Valley Memorial System, including but not limited to user's electronic files, e-mail messages, instant messaging, Internet usage, voice mail messages, and text messages.

- Incidental Personal Use: Yakima Valley Memorial's systems are for business use. Limited, occasional or incidental use of these tools for personal purposes is permitted during off-duty time (rest breaks, meal breaks, before/after a shift) and must not interfere with Yakima Valley Memorial's patient service standards or other performance standards.

APPROPRIATE ELECTRONIC COMMUNICATIONS

Electronic communications can be forwarded, intercepted, printed and stored by others; therefore user will use professional language and apply discretion with regard to the information included in electronic communications.

Use of Yakima Valley Memorial Email:

- Forwarding or electronically posting Yakima Valley Memorial's internal communications or proprietary information to individuals outside of Yakima Valley Memorial is not permitted.
- Email will not be used to communicate protected health information (PHI) with patients. Electronic communication containing PHI must be conducted through patient portals provided by Yakima Valley Memorial.
- Email correspondence with patients not containing PHI, such as sending a blank form, may be sent via email, provided the patient is not requested to return the completed form electronically.
- Email can be used to communicate with Yakima Valley Memorial business partners who have Yakima Valley Memorial approved secure email communications such as Transport Layer Security (TLS). See Memorialnet for list of business partners with secure email communication, listed on Information Security and Privacy department page.
- Email footers and signature blocks should generally be used to provide the author's name, title, and telephone number. Signature blocks may not contain commercial, political, religious, or inappropriate references and must be consistent with this policy.
- Emails from senders that are not known or expected by the recipient should be considered suspicious. Do not open any attachments or click on any web links in the email; instead view in the Outlook preview pane. Contact the IS Help Desk for assistance validating suspicious emails.
- Yakima Valley Memorial's email system is the only authorized email system to conduct Yakima Valley Memorial business. Do not use any other email system to conduct Yakima Valley Memorial business.
- Use of email for marketing, promotional or newsletter distribution purposes is only permitted with approval from the Yakima Valley Memorial Communications and/or Marketing Departments.
- Forwarding email or other communications from in-house attorneys or outside legal counsel, or the contents of that email, to individuals either inside or outside of the company is not permitted without the express authorization of counsel.
- Attempting to obtain or obtaining access to the email records or electronic communications of others with no permissible company business purpose is not permitted.

Social Media (Business and Personal):

- All business-related social media must comply with organizational communication guidelines. Contact Yakima Valley Memorial Communications for more information.
- When communicating using the Internet about Yakima Valley Memorial or Yakima Valley Memorial-related matters, the user must disclose their connection with Yakima Valley Memorial and their role.
- The user should write in the first person and make clear they are not speaking on behalf of Yakima Valley Memorial. In those circumstances the user should include a disclaimer such as, "the views expressed on this blog or website are my own and do not reflect the views of my employer."
- The user must use a personal email address, not their Yakima Valley Memorial email address, as the means of identification.
- If users have questions about what is appropriate to include in their blog or social networking profile they should contact Yakima Valley Memorial Communications.

Telephone and Mobile Device Use:

- Users must use off-duty time (rest breaks, meal breaks, before/after a shift) to make personal telephone calls or engage in personal text messaging.
- Except for approved business processes, cell phones will be stored out of public view in areas with patient interaction, as they may inappropriately interrupt patient care, customers or co-workers. Under no circumstances should users engage in personal text-messaging in view of patients.
- Users are required to ensure coverage of work duties in the event they must make a personal call.
- When job duties necessitate taking photos, users must follow the Yakima Valley Memorial Photographic, Video and/or Audio policy and standard processes.

The following electronic communications activities are not permitted, using Yakima Valley Memorial Systems:

- Sending any communications or engaging in activities, such as chain letters, pyramid schemes, gambling or any other activity in violation of local, state, or federal law;
- Sending, receiving, or soliciting offensive, sexually-explicit, or harassing statements, images or language including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs;
- Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing;
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication;
- Soliciting funds or services for charitable causes that are not Yakima Valley Memorial - sponsored or without prior approval from The Memorial Foundation.
- Using non-Yakima Valley Memorial provided cloud file sharing sites unless formally reviewed and approved by Virginia Mason Information Systems

PROTECTING OUR ASSETS

A. Information Assets:

- All Yakima Valley Memorial protected health or proprietary information must be stored on network servers. Unless specifically approved by the Chief Information Security Officer neither Yakima Valley Memorial PHI or Yakima Valley Memorial proprietary information shall be stored unencrypted on mobile devices or other removeable media. In addition, PHI shall be secured by means of data encryption as required by law.

- Users must take all reasonable precautions to prevent the loss or theft of Yakima Valley Memorial computers, mobile devices, USB drives, Yakima Valley Memorial portable media, ePHI and other information assets on any media.
- Disclosing, sending, receiving, printing, or otherwise disseminating proprietary information, trade secrets, or confidential information in violation of Yakima Valley Memorial's confidentiality, privacy and security policies, or local, state, or federal law is prohibited.
- Copying or transmission of any document, software or other intellectual property protected by copyright, patent or trademark law, without proper authorization by the owner of the intellectual property is not permitted.
- Copying, disseminating, or reproducing information on the Internet that has been authored by others without the express permission of the author or copyright holder(s) is not permitted.
- Disclosure of protected health and proprietary information without appropriate authorization, or for a use that is not otherwise permitted is prohibited.
- Using, transmitting, changing, or deleting another user's files, documents, software, or other media without the User's or manager's permission is prohibited.

B. Computing and Technology Assets:

- Only Yakima Valley Memorial Information Systems' owned and/or managed devices, such as printers, servers, routers, switches, firewalls, wireless access points, external hard drives, etc., may be connected directly to the Yakima Valley Memorial business network.
- The purchase or implementation of any application, (packaged, homegrown, smart phone application or web application), that will be used to support the business of Yakima Valley Memorial must be evaluated by Information Systems.
- Gaining access to Yakima Valley Memorial's facilities, systems, content, or infrastructure by using any access-control mechanism not assigned to the particular user ("impersonating"), or permitting another person to have access by sharing one's Yakima Valley Memorial credentials and passwords is prohibited.

Any user who learns of the loss or theft of a computer or other information asset will immediately notify their supervisor, submit a Patient Safety Alert and contact the Chief Information Security and Privacy Officer.

PROTECTING OUR BUSINESS COMPUTER ENVIRONMENT

A. Managing Resources Wisely:

Users must not over-burden Yakima Valley Memorial's systems such as saving unnecessary or non-work related files, streaming media, downloading unauthorized programs, exposing Yakima Valley Memorial to allegations of copyright infringement, or introducing viruses. To that end, users MUST NOT:

- Disable, alter or circumvent any device or software utility, or configuration parameters installed by Yakima Valley Memorial Information Systems;
- Upload or send any file or program saved on any removable media or other device originating from a computer outside the Yakima Valley Memorial network without contacting Information Systems to ensure that the disk, file, or program is free of any virus or other destructive file or program and meets Information System's standards;
- Attempt to download or stream external music, movies, etc., on the Yakima Valley Memorial network;

- Discard removable media including CDs, DVDs, VHS tapes, cassettes, memory cards and USB drives that may contain protected health or proprietary information without following the standards for media destruction and sanitization consistent with requirements established by Information Systems;
- Engage in open, unencrypted transmissions containing ePHI.

B. Protecting Against Malware and Social Engineering:

Users must exercise caution to avoid the introduction of computer viruses or other destructive files or programs into Yakima Valley Memorial Systems. At a minimum, users must not:

- Download or open email attachments from unknown senders;
- Download or install unapproved software without the assistance of Yakima Valley Memorial Information Systems;
- Download files from the Internet without being sure of a file's security authenticity;
- Disable any antivirus controls installed by Yakima Valley Memorial Information Systems.
- Introduce malware, including viruses, worms, adware, spyware, keystroke loggers, and root kits into any Virginia Mason System;
- Install, implement or use peer-to-peer systems on Yakima Valley Memorial computers;
- Use systems or technology that disguise or alter the identifying information of the computer user, such as external proxies or anonymizer sites, for any purpose;
- Browse or download content from Internet sites containing sexually-oriented images or information, gambling content, content associated with violence or hate, spyware and hacking tools, or criminal activity, whether or not the content is blocked;
- Use external instant messaging.
- Subscribe to non-business-related internet web feeds and mailing lists.

C. Enhancing Security Through Passwords:

Access to Yakima Valley Memorial Systems is only for authorized users. Users will comply with the following:

- Passwords and other access-control tools must not be shared with anyone - including the Help Desk, co-workers or managers.
- Passwords and log-on information must not be publicly posted in any manner or format, and must not be left in an unsecured location, such as under a keyboard, on a monitor, calendar or desktop.
- All authorized users will be issued a temporary password. The first time a user logs into a system they will be prompted to change that password to something they select and keep private.
- Passwords must be at least eight characters in length and should contain both letters and numbers and at least one nonstandard character (@, #, $, &, *, etc.). Additionally, passphrases may be used, e.g., patiytu76 (Put A Tiger In Your Tank Union 76).
- Words found in the dictionary should not be used as passwords.
- For certain applicable systems, multiple failed logon attempts may result in an account lock-out requiring an account reset.
- **If a user believes his/her password or any other access control tool has been compromised, the user must immediately change the password and contact the Yakima Valley Memorial IS Help Desk (509.575.8175).**

RESPONSIBLE USE AUDITS

Yakima Valley Memorial reserves the right to audit any Yakima Valley Memorial system to support the identification and termination, of unauthorized activity.

VIOLATIONS

Violations of this policy may result in disciplinary action including termination of email or Internet privileges, termination of employment, and/or referral of the user to law enforcement authorities for local, state and federal offenses.

Users are required to report all suspected policy violations through any of the following means:

- Immediate supervisor
- Human Resources
- Integrity Hotline
- Patient Safety Alert System
- Privacy Officer
- Chief Information Security Officer

Nothing in this policy will limit authorized Human Resources or Legal Department staff from taking action, or requesting information, as necessary to comply with any legal obligation or their job duties. Actions taken under the direction of authorized Yakima Valley Memorial Staff to protect Yakima Valley Memorial Systems will not be a violation of this policy.

EXCEPTIONS

Exceptions to this policy may be granted in unusual or special circumstances. Exceptions are only granted with the written approval of the Chief Information Security Officer and Human Resources. Security standards are subject to exception only when it would not be reasonable and appropriate to implement the standard and where equivalent measures are not reasonable and appropriate under the circumstance.

DEFINITIONS:

Refer to Yakima Valley Memorial Policy Development & Approval - Appendix A for standard workforce, roles and work product definitions.

Access control: a process by which users are granted access and certain privileges to systems, resources or information. Examples of access control tools include passwords, multi-factor authentication and proximity badges.

Chief Information Security Officer: the person responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that protected health information, information assets and technologies are adequately protected.

Computer Network: the local and wide area networks, computers, communication devices, software systems, applications, e-mail, and other systems operated by or on behalf of Yakima Valley Memorial that are used to enable Yakima Valley Memorial and users to store, process, and use information in electronic form, and to facilitate communications among members of the workforce and to third parties.

Confidential Information: includes any of the following:

- Protected Health Information (ePHI)
- Personal Identifiable Information (PII)

Confidentiality: protecting information from unauthorized use or disclosure.

Electronic Communication Tools: the computer network and any computing solution including but not limited to the following: pager, phone, cell phone, mobile devices, computer, laptop, software applications, web applications, smart-phone applications, fax machines, social media etc.

Electronic Communication: any information transmitted via an electronic communication tool as defined herein.

HIPAA: Title II of the Health Insurance Portability and Accountability Act of 1996 (Pub. Law 104-91) and implementation of regulations issued by the Secretary of Health and Human Services found at 45 CFR Parts 160 – 164.

Malware: malicious software, is hostile or intrusive software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems and exist in a variety of forms, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Individually Identifiable Information: information that identifies an individual, or which might be used to identify an individual including the individual's name, address, names of relatives, employer, date of birth, telephone or fax number, e-mail address, social security number, patient identification number, certificate or license number, web URL, IP address, finger and voice prints, photographic image or other unique identifying number, characteristic or code.

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 Privacy Rule compliance.

Proprietary Information: trade secrets and information about the business plans, marketing plans, costs, contracts, financial information, or operations of Yakima Valley Memorial that are not in the public domain and which access to, use and disclosure of must be controlled by Yakima Valley Memorial.

Protected Health Information (PHI): any individually identifiable information which is health information that identifies an individual as a recipient of physical or mental health services; or relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual; or the past, present or future payment for the provision of health care services to an individual. The definition applies to information transmitted or maintained in any form or medium, including electronic, paper, and oral. The privacy protections of HIPAA apply to PHI. PHI does not include educational records governed by Family Educational Rights and Privacy Act, and employment records.

Restricted Areas: A designated space in a surgical suite that can only be accessed through a semi-restricted area in order to achieve a high level of asepsis control. Traffic in the restricted area is limited to authorized personnel and patients, and personnel are required to wear surgical attire and cover head and facial hair. Masks are required where open sterile supplies or scrubbed persons may be located. A ***semi-restricted area*** comprises the peripheral support areas surrounding the restricted area of a surgical suite. These support areas include facilities such as storage areas for clean and sterile supplies, sterile processing rooms, work areas for storage and processing of instruments, scrub sink areas, corridors leading to the restricted area, and pump rooms.

Secure: Content which is protected through encryption.

Social Engineering: psychological manipulation of an individual, intended to steer the person into divulging confidential information, or performing actions allowing for computer system access. Social engineering generally involves fraudulent representations.

Systems: the computer network and any electronic communication tool as defined herein.

User: any member of Yakima Valley Memorial's workforce and others who access, utilize, modify or otherwise manipulate information stored on computer or other electronic systems operated by Yakima Valley Memorial, whether such use is on Yakima Valley Memorial property or not.

Yakima Valley Memorial (YVM): Yakima Valley Memorial is the parent company of a group of affiliated organizations including Memorial Physicians PLLC

REFERENCES:

Policies:

Privacy of Confidential Information
Workforce Privacy and Security Training and Agreement
Photographic, Video and/or Audio Recordings Policy and Standard Process
Yakima Valley Memorial Social Media Guidelines

Tools:

Health Insurance Portability and Accountability Act of 1996 and implementing regulations
The Joint Commission Information Management Standards and Elements of Performance

KEYWORD Indexes: Social media, cloud storage, password, personal devices, computer, HIPAA

Effective Date:	June 9. 2020	**Term Date:**	JMay 2023
Governing Department:	Information Security Communications Human Resources		
Sponsor:	Ellen Wiegand, VP, Chief Information Officer		
Authored By:	Ellen Wiegand, VP, Chief Information Officer	**Date:**	January 2020
Review By:	Policy Reliability Workgroup	**Date:**	April 2020

POLICY

Approved By:	Information Security Oversight Committee	**Date:**	May 2020
Approved By:	Senior Leadership Team	**Date:**	June 2020
Next Review Date:	May 2023		

Paper copies of this document may not be current and should not be relied on for official purposes. The current version is on the organization intranet.