UMass Memorial Health

Policy

Acceptable Use of Electronic Resources

Developed By: HIPAA Advisory Group & Privacy and Security Committee	**Effective Date:** 8/12/2021
Policy Owner: Bruce Forman	**Approved by:** Robin Sodano, Vice President, Chief Information Officer **Approved by:** Eric Dickson, MD, CEO, UMass Memorial Health
Applicability: This policy applies to Workforce Members who use UMass Memorial Health (UMMH) Electronic Resources and personal devices that connect to the UMMH network	

Keywords: acceptable use, Electronic Resources, PHI, PI, email, internet, data use, wireless devices, prohibited use, information security, privacy

Policy

UMass Memorial Health (UMMH) Workforce Members must only use Electronic Resources as permitted by this policy.

This policy defines the boundaries for the “acceptable use” of UMMH Electronic Resources, including software, hardware devices and network systems; and for the acceptable use of non-UMMH owned devices used to access UMMH Electronic Resources. This policy is intended to promote employee productivity and safety while recognizing that technology alone cannot protect against internal and external threats to UMMH resources and assets. Other intentions of this policy include:

- Protect Patient, Employee, and UMMH Confidential Information including Protected Health Information (PHI) and Personal Information (PI).
- Maintain compliance with applicable state and federal laws and regulations, including, but not limited to, Health Insurance Portability and Accountability Act ("HIPAA") and Massachusetts Data Security Regulations.
- Protect Workforce Members from discrimination and harassment.
- Prevent copyright infringement, software piracy, and other misuse of UMMH Electronic Resources.
- Protect UMMH against computer crimes, viruses, hackers, pranks, Denial of Service attacks, cyber terrorism, and other civil and criminal wrong doings.
- Restrict use of UMMH Electronic Resources to acceptable UMMH uses as defined in this policy.
- Workforce Members must have no expectations of privacy in anything they create, store, send or receive on UMMH Electronic Resources.

This Acceptable Use Policy provides guidance related to the use of, but is not limited to, the following types of technology:

Email	Camera/Video/Photos
Text/Instant Messaging	Internet

Voice mail	Servers
Desktop/Workstations	Software
Mobile Devices	Computer networks (wired, mobile and wireless)
Telecommunication Devices	Printers
Data Storage Devices	

Definitions

Computing Devices – devices that have been evaluated and accepted by Information Services as compatible with the network and that have approved software and security controls installed. Computing Devices include Workstations, Mobile Devices, Data Storage Devices, Printers and Network Devices.

Confidential Information – data/information (whether in oral, written, printed, electronic or any other form) related to the business of UMMH (including but not limited to PHI, PI, finance and administration, human resources, legal, clinical, and any other patient and research data), that is not freely disclosed; private information that is entrusted to another with the confidence that unauthorized disclosure will not occur.

Cyberbullying - is a form of bullying or harassment that is perpetrated using electronic forms of contact. Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Data Storage Device – a device for recording (storing) information (data). A storage device may hold information, process information, or both. Data Storage Devices include, but are not limited to, portable hard drives, USB drives, flash drives, and DVDs.

Electronic Resources – includes all information technology related software, devices, systems, and media, including Computing Devices, Peripheral Devices, Telecommunication Devices, and Wireless Access Points, either owned or managed by UMMH, or accessed via FMD or Webmail.

Follow Me Desktop (FMD) – UMMH's software application that allows authorized Workforce Members to access the UMMH network from a remote location.

Intellectual Property – property rights created through intellectual and/or discovery efforts of a creator that are generally protectable under patent, trademark, copyright, trade secret, trade dress (e.g. the appearance or image of a product) or other law.

Malicious Intent – includes but is not limited to any intentional act that knowingly violates UMMH policies and/or local/state/federal laws and regulations as well as hacking, cracking, bugging, virus creation/propagation, tampering with government or private data without authorization, and the intentional non-secure transmission of sensitive data across the internet or other non-secure network.

Managed Device – any Computing Device, Peripheral Device, Telecommunication Device or Wireless Access Point that is either owned by UMMH or not owned by UMMH, but is:

- Registered, approved and authorized by UMMH to access, transmit or store UMMH information for purposes of conducting UMMH business, and
- Configured to meet UMMH's standards for security control, including as technically appropriate for a device, but not limited to:
    - Centrally managed,
    - Encrypted,
    - Protected by anti-virus/malware software, and
    - Capable of having UMMH content remotely wiped/deleted from the device.

Devices that are not owned by UMMH which are Managed Devices may have a portion of the device that is managed and another portion of the device that is non-managed. For example, a personally owned smartphone may have software installed by UMMH that segregates and protects UMMH information to one part of the smartphone, without interfering with the user's personal information on another part of the smartphone. Where this is the case, the term "Managed Device" will only apply to that portion of the device that is managed by UMMH.

Mobile Device – an easily portable device that combines computing, telephone/fax, email and networking features. Examples of Mobile Devices include smartphones and tablets.

Network Devices – are components, such as routers, switches, firewalls, and servers, used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines.

Non-Managed Device – is a non-UMMH device or personally owned device that has not been registered, approved and authorized by UMMH. Non-Managed Devices may only connect to the guest wireless network, FMD and Webmail.

Personal information (PI) – an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Peripheral Devices – devices connected to Computing Devices to provide additional functions, such as printing, copying, scanning, faxing and storing information. Examples of Peripheral Devices include copiers, fax machines, printers, scanners and multifunction machines.

Protected Health Information (PHI) – information created, transmitted, received, or maintained by the UMMH Organized Health Care Arrangement (OHCA), including demographic information, related to the:

- Past, present, or future physical or mental health or condition of an individual;
- Provision of health care to an individual; or
- Past, present, or future payment for the provision of health care to an individual; **together with** any of the identifiers in the list below.

Names (of patients, relatives, or	Social security numbers	Device identifiers and serial numbers
All geographic subdivisions smaller	Medical record numbers	Web Universal Resource Locators
All elements of dates (except year) including birth date, admission date, discharge date, date	Health plan beneficiary numbers	Internet Protocol (IP) address numbers
Telephone numbers	Account numbers	Biometric identifiers, including finger and
Fax numbers	Certificate/license numbers	Full face photographic images and any
Electronic mail addresses	Vehicle identifiers and serial numbers, including license	Any other unique identifying number, characteristic, or code

- PHI does not include information maintained about an individual by a UMMH entity for employment purposes, such as employee health records.

- Note: Information for deceased individuals continues to be PHI until the individual has been deceased for more than 50 years.

Telecommunication Devices – a device used for the electronic transfer of information from one location to another. Telecommunications or telecom refers to a mix of voice and data, both analog and digital. Examples of Telecommunication Devices include telephones, mobile phones, smartphones, and pagers.

Text Messaging, or Texting – the exchange of brief Text Messages between mobile and/or smartphones.

Trusted Email Domain – an email domain of an entity outside of UMMH, for example umassmed.edu and healthalliance.com for which UMMH has established a permanently encrypted connection for the purpose of sending and receiving email messages.

Webmail – UMMH's software application that allows individuals with a UMMH email account to access the UMMH email network from a remote location.

Wireless Access Points - is a networking hardware device that allows a Wi-Fi enabled device to connect to a wired network.

Workforce Members – All employees, contractors, volunteers, trainees (including medical students, interns, residents, allied health professionals and business students), members of the medical staff including employed and private physicians, nurses in expanded roles, physician assistants, temporary employees, and other persons employed, credentialed or under the control of UMMH whether or not they are paid by UMMH.

Workstation - any desktop computer, VDI thin client, or laptop. In this context, Workstation is a generic term for a user's machine used for UMMH work. It may include one or more displays and other Peripheral Devices such as a printer, monitor, external hard drive, etc.

Required Criteria for Procedure

A. General Provisions

1. All data created by Workforce Members on UMMH systems is the property of UMMH.
2. UMMH owned Electronic Resources are only for use by Workforce Members.
3. UMMH Electronic Resources will be used in compliance with applicable organizational policies, standards, guidelines, state and federal regulations and laws.
4. Workforce Members are to honor and respect all applicable intellectual property including, but not limited to:
   a. Software
   b. Discoveries
   c. Web content materials
   d. Licenses
   e. Digital certificates
5. Workforce Members using FMD to print when either on or off site must follow UMMH Privacy and Information Security policies regarding physical security to prevent the printed material from being inappropriately disclosed. For Workforce Members working remotely, extra precautions should be taken regarding printed materials which include, but are not limited to, shredding unneeded printed documents using a crosscut shredder and once a Workforce Member is no longer working on a printed document and at the end of the work day, securing the printed document under lock and key until it needs to be destroyed. Printed materials that contain PHI, PI and Confidential Information must be shredded using a crosscut shredder when no longer needed and stored under lock and key when a Workforce Member is no longer working on a printed document and at the end of the work day, until it needs to be destroyed. Some printed

material may constitute UMMH records. Please see the UMMH Records Retention and Destruction Policy for information.

B. Managed Devices

1. Only Managed Devices may be used to store, process and/or transmit data used to support the clinical, administrative, research, educational and other business functions of UMMH, or be connected to UMMH systems or networks other than as permitted by Section C.1. below.
2. Users of Non-Managed Devices may submit a request to have the device become a managed device by submitting an *Exception to Desktop* form. Contact the Support Center for an electronic copy of the *Exception to Desktop* form.
3. If security controls are not already present, Workforce Members will work with Information Services to install UMMH security controls on Managed Devices. Security controls may include as technically appropriate for a device, but will not be limited to, the following:
   a. PIN
   b. Lockout setting
   c. Encryption
   d. Virus Protection on laptops and desktops
   e. Remote wipe for smartphones and tablets

   Open a ticket with the Support Center to request assistance from Desktop Services.
4. Computer programs will not be installed onto any UMMH Managed Device without I.S. approval and the installation may only be performed by approved individuals.
5. Managed Devices must not be in an altered state such as “Jailbroken” iPhones or ‘Rooted’ Android devices.
6. Any Managed Device that is lost or stolen must be reported immediately to the I.S. Support Center.
7. When a Workforce Member leaves or is terminated, or if the Workforce Member chooses to stop connecting his/her managed device to the UMMH network, UMMH data stored on the device must be removed (wiped) from the device by calling the I.S. Support Center.
8. Device Reuse or Termination of Employment: To dispose of or reuse a Managed Device, Workforce Members must open a ticket with the Support Center. Information Services will determine the appropriate process to disable access to the UMMH network and to assure the secure removal of any UMMH information that may be on the Managed Device prior to disposal or reuse. Only performing a standard delete function may not be sufficient to cleanse the data. Desktop Services will update its inventory of Managed Devices to note the removal of a Managed Device from the UMMH network.
9. Sending UMMH Confidential Information to UMMH display pagers is allowed, but message senders must limit confidential content to the minimum information necessary, and pagers must never be used to transmit patient care orders.
   a. Use of messaging through the electronic health record is the preferable communication method for non-urgent UMMH Confidential Information.

C. Non-Managed Devices

1. Non-Managed Devices may connect to the UMMH guest network, FMD and Webmail.
2. Workforce Members using Webmail must follow the following safeguards:
   a. Never open attachments when using Webmail, since the attachments may be saved to the Non-Managed Device used to open Webmail.
   b. Never save email or attachments when using Webmail.
3. Never save UMMH Confidential Information to a Non-Managed Device.

D. Workstation Use

1. Workforce Members will use the workstation locking capability (CTRL-ALT-DEL) whenever leaving their workstation unattended. (Remember: “Control, Alt, Delete, when leaving your seat.”)
2. Remote control connection from one workstation to another, such as that used by Information Services for remote troubleshooting, must be disconnected by the party that remotely connected to the workstation after the session is completed.
3. Workforce Members will log off from their workstation(s) when their shifts are complete.

E. Physical Security

1. Laptops, Mobile and Data Storage Devices must be kept in the physical presence of the user or when left unattended on site stored out of sight in a locked office, locked drawer, locked closet, or cable lock. When taken off site, laptops, Mobile and Data Storage Devices must be kept in the physical presence of the user or when left unattended locked out of sight such as in a car trunk, home, or hotel room safe. Laptops, Mobile and Data Storage Devices must be moved to the most secure site available at any given time. For example, a device must be removed from a car trunk when a user arrives at his/her home and secured in the locked home.
2. Workstations that are not laptops that are located on site in publicly accessible places will have device locks installed.

F. Email and Text Activities

1. Email and other electronic material may constitute UMMH records. Please see the UMMH Records Retention and Destruction Policy
2. Email transmissions, both on the intranet and the internet, may be subject to disclosure through legal proceedings or as otherwise required by law.
3. Some messages sent, received or stored on the UMMH email system may constitute privileged communications between UMMH and its in-house or external attorneys. If you receive an email labeled “Privileged Attorney-Client Communication” (or similar language), you should seek the attorney’s permission before disseminating it further, as the privilege may be destroyed if the transmission is sent to a third party.
4. Always encrypt emails when sending emails containing Confidential Information outside the UMMH trusted email domain. Emails are sent encrypted when the word **secure** is in the Subject line of the email. Be certain to always double-check all “to” and “cc” fields prior to sending any emails to determine if any recipients are outside of the trusted email domain. A list of trusted email domains may be found here: (Link to Be added) **Limited exception:** An individual may request to have their PHI sent unencrypted. Please see the Uses and Disclosure of Protected Health Information Policy for more information about this exception and required accompanying process.
5. Confidential Information may be transmitted via email within UMMH with minimal risk.
6. When conducting UMMH business, Workforce Members may only use their UMMH email accounts. Use of a non-UMMH email account, such as a Gmail, Hotmail, or an account provided by another entity, is not permitted. UMMH email must never be forwarded automatically to a non-UMMH account.
7. Occasional use of UMMH email and electronic resources for personal reasons is permitted.
8. Text Messages are not encrypted and therefore may not be used to transmit PHI. Use messaging through the electronic health record for messages containing PHI.

G. Internet Use

1. The internet and all UMMH electronic resources are to be used primarily in support of UMMH related patient care, business, and research activities.
2. All copyright laws and regulations are in effect in the online environment.
3. Users who violate copyright and/or license terms are personally liable for their actions.
4. UMMH utilizes an Internet content filtering tool which prohibits access to sites, including, but not limited, those in the categories of:

Adult	Instant Messenger
Anonymizer	Nudity
Browser Toolbar (e.g. Google Toolbar)	Pop Up Web Advertisements
Dating	On-Line Gaming
File Sharing Sites	Pornography
Gambling	Spyware/Malicious Sites
Hate and Racism	Streaming Radio
Illegal Chat	Weapons

Inactive Sites	

5. UMMH recognizes Workforce Members need to share documents with external users. Although email is a good method for communication, it is not always the best method for file sharing. Drop Box is a file sharing site that UMMH has approved for file sharing purposes. However, sharing files on Drop Box is only acceptable for de-identified data, resumes, presentations, or any document which does not contain UMMH Confidential Information or Intellectual Property.

H. Passwords and Device Authentication

1. Individual passwords must be kept secret, never shared with anyone for any reason. Exceptions must be approved by the Chief Information Security Officer. If written down, passwords must be stored in a locked drawer or cabinet to which only the user has access. Passwords must not be stored electronically other than within a UMMH provided single-sign on solution.
2. Never permit another user to establish a biometric identifier that is used in place of a password to provide access to a Managed Device that contains UMMH information.
3. All users will adhere to the proper procedures for accessing UMMH's network, including the use of access tokens where indicated and strong passwords that are to be changed periodically. Refer to Information Services Procedure/Standard/Guideline 05.06 Password Administration & Management

I. Prohibited Activities

Use of UMMH Electronic Resources for the following purposes is prohibited:

1. Activity with malicious intent; procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws; activities disruptive to the operation of UMMH business; disparagement of others; advocating or opposing political, religious or cultural agendas; or for personal gain (as in the use of chain letters requesting donations).
2. Creation or transmission of any offensive, obscene or indecent images, data or other material.
3. Storage or indexing of UMMH information on an external site (e.g. desktop search engines, Google docs) without the knowledge and approval of Information Security Team and the benefit of a fully executed contract between UMMH and the third party.
4. Sending Confidential Information outside the UMMH network without encryption. (This prohibition does not include the exception noted in the Uses and Disclosures of Protected Health Information Policy).
5. Violations of the rights of any person or company protected by copyright, trade secret, patent or other Intellectual Property, or similar laws or regulations, including, but not limited to, the installation, distribution or digitization of "pirated" or other software products, photographs, music, magazines, books, or other copyrighted material, that are not appropriately licensed for use by UMMH.
6. The intentional introduction of malicious programs onto UMMH systems or networks (e.g. viruses, worms, Trojan horses, email bombs, etc.).
7. Making fraudulent offers of products, items or services originating from any UMMH account.
8. Intentionally causing security breaches or disruptions of any system or network, including but not limited to disruption for malicious purposes. Security breaches include, but are not limited to, accessing data for which the Workforce Member is not an intended recipient or authorized to access, or logging into a server or account that the Workforce Member is not expressly authorized to access, unless such access is within the scope of regular duties.
9. Transmitting or forwarding Confidential Information to outside companies or individuals not authorized to receive such information, or to UMMH employees who have no business or clinical reason for such information.
10. Using security assessment software, such as port scanning or network vulnerability scanning unless conducted by Information Security staff or other personnel authorized by UMMH Information Security Management.
11. Executing any form of network monitoring which will intercept data not intended for the Workforce Member's Computing Device unless this activity is a part of the Workforce Member's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.

13. Providing information about, or lists of, UMMH patients or Workforce Members to unauthorized parties outside UMMH unless authorized by UMMH management.
14. Any activity that is disruptive to the operation of UMMH business.
15. Posting non-business-related messages to Usenet or Listserv servers.
16. Installing computer hardware or software on UMMH Electronic Resources, including personal software and data without the approval of Information Services.
17. Downloading, file sharing, or storing UMMH Confidential Information outside the UMMH network except as authorized by the Chief Information Security Officer.
18. Using UMMH email accounts, including email usernames and passwords for the following, if they are not business related:
    a. Chat rooms/blogs/forums
    b. Bulletin boards
    c. Instant messaging
    d. Peer-to-peer file transfers (such as music downloads or other non-business applications)
19. Saving, forwarding or sending email chain letters, hoaxes, or pranks.
20. Viewing another user's email without permission; sending, creating, monitoring or receiving email or other information or material under another user's username or tampering with, revealing, or changing another user's password.
21. Auto-forwarding UMMH email to an outside email account due to the potential negative impact on servers and to protect Confidential Information from being sent over the internet in an unsecure manner.
22. Sending unsolicited email messages, including the sending of "junk mail" or other advertising materials (email spam).
23. Forging unauthorized email header information.
24. Enrolling any email address, other than the email address of the user, in a system that automatically sends email content to the enrollee.
25. Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
26. Cyberbullying or posting/distributing discriminatory content is prohibited.
27. Using UMMH Confidential Information for any unauthorized purpose or activity which violates the rights of privacy of UMMH patients and Workforce Members. Refer to Breach of Confidential Information policy.

J. Monitoring, Enforcement, Corrective Actions and Discipline

1. In order to assure the security of UMMH Confidential Information and compliance with this policy, UMMH actively monitors activity on its Network and of its Managed Devices. UMMH may monitor or review any data stored on Managed Devices at any time. UMMH may also monitor devices that are Non-Managed Devices that are only using FMD or Webmail, but only as it relates to their use of FMD or Webmail. Data and activity that may be monitored and reviewed include, but are not limited to:
    - Email sent and received
    - Patient-centered messages sent within the electronic medical record
    - Internet usage,
    - Files, documents and faxes created, stored, deleted or distributed,
    - Voice mail and messages,
    - UMMH Confidential Information, and
    - Software, or applications owned or licensed to UMMH.
2. Workforce Members should understand that computer activities create audit trails, and that deleted, edited and overwritten computer files often cannot be erased or may be recovered using computer forensic techniques.
4. Workforce Members must have no expectations of privacy in anything they create, store, send or receive on UMMH Electronic Resources, including on UMMH owned or Managed Devices, or when using FMD or Webmail.
5. Any Workforce Member using UMMH Electronic Resources does so subject to UMMH's rights to monitor such use and are advised that if monitoring reveals possible evidence of criminal activity, UMMH may provide this information to law enforcement officials.

6. Workforce Members must report any suspected and/or known violation of this Acceptable Use Policy to the Privacy and Information Security Office (privacyandsecurity@ummhc.org) or through EthicsPoint (umassmemorial.ethicspoint.com or 844-744-9212).
7. UMMH reserves the right to revoke any user's access privileges at any time for violations of this policy, any other UMMH policy, or conduct that disrupts the normal operation of UMMH's information systems.
8. Violations of this policy could result in the permanent removal of ALL data, without notice, residing on Managed Devices and Non-Managed Devices.
9. Violations of this policy can result in disciplinary action, up to and including immediate termination and/or legal action.

Entity/Department Specific Procedures

N/A

Supplemental Materials

N/A

Rescission

Supersedes policy dated: 1/29/20

References

Written Information Security Policy
Breach of Confidential Information
Uses and Disclosure of Protected Health Information Policy
Policy 1428 Social Networking
Performance Management/Discipline
Sexual Harassment
Corporate Compliance: Code of Ethics and Business Conduct
Joint Commission Perspectives, Clarification: Use of Secure Text Messaging for Patient Care Orders is Not Acceptable; **December** *2016.*