UMass Memorial Medical Center
Policy

1425 Acceptable Use of Electronic Resources	
Developed By: HIPAA Advisory Group & Privacy and Security Committee **Policy Owner:** Bruce Forman	**Effective Date:** 1/25/2017 **Approved by:** Patrick L. Muldoon, FACHE President, UMass Memorial Medical Center
Applicability: This policy applies to workforce members who use UMass Memorial electronic resources and personal devices that connect to the UMass Memorial network	**Rescission: Supersedes policy dated:** 6/4/12
Keywords: acceptable use, electronic resources, PHI, PI, email, internet, data use, wireless devices, prohibited use, information security, privacy	

I. Policy:

UMass Memorial workforce members must only use Electronic Resources as permitted by this policy.

This policy defines the boundaries for the "acceptable use" of UMass Memorial Medical Center's (UMass Memorial) electronic resources, including software, hardware devices and network systems; and for the acceptable use of non-UMass Memorial owned devices used to access UMass Memorial 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 UMass Memorial resources and assets. Other intentions of this policy include:

- Protect Patient, Employee, and UMass Memorial 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 UMass Memorial electronic resources.
- Protect UMass Memorial against computer crimes, viruses, hackers, pranks, Denial of Service attacks ("DOS"), cyber terrorism, and other civil and criminal wrong doings.
- Restrict use of UMass Memorial electronic resources to acceptable UMass Memorial uses as defined in this policy.
- Workforce members must have no expectations of privacy in anything they create, store, send or receive on UMass Memorial electronic resources, on managed devices, or when using FMD or webmail.

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

- Email
- Text/instant messaging
- Voice mail
- Internet
- Servers
- Desktops/workstations
- Mobile devices
- Telecommunication devices
- Data storage devices
- Software
- Computer networks (wired, mobile and wireless)

II. 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, and network devices.

Confidential information – data/information (whether in oral, written, electronic or any other form) related to the business of UMass Memorial (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.

Follow Me Desktop (FMD) – UMass Memorial's software application that allows authorized workforce members to access the UMass Memorial 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 UMass Memorial 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 UMass Memorial or not owned by UMass Memorial, but is:

- Registered, approved and authorized by UMass Memorial to access, transmit or store UMass Memorial information for purposes of conducting UMass Memorial business, and
- Configured to meet UMass Memorial'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 UMass Memorial content remotely wiped/deleted from the device.

Devices that are not owned by UMass Memorial 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 UMass Memorial that segregates and protects UMass Memorial 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 UMass Memorial.

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-UMass Memorial device or personally owned device that has not been registered, approved and authorized by UMass Memorial. Non-managed devices may only connect to the guest wireless network, FMD and web mail.

Personal information (PI) – refer to Privacy and Information Security definitions.

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) – refer to Privacy and Information Security definitions.

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 written text messages between mobile and/or smartphones.

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

Web Mail – UMass Memorial's software application that allows individuals with a UMass Memorial email account to access the UMass Memorial 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 – refer to Privacy and Information Security definitions.

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

III. General Procedure:

A. General Provisions

1. All data created by workforce members on UMass Memorial systems is the property of UMass Memorial.
2. UMass Memorial owned electronic resources are only for use by workforce members.
3. UMass Memorial 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

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 UMass Memorial, or be connected to UMass Memorial 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 UMass Memorial 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 UMass Memorial 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 an employee leaves or is terminated, or if the employee chooses to stop connecting his/her managed device to the UMass Memorial network, UMass Memorial 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 UMass Memorial network and to assure the secure removal of any UMass Memorial 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 UMass Memorial network.
9. Sending UMass Memorial confidential information to UMass Memorial 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.

C. Non-Managed Devices

1. Non-managed devices may connect to the UMass Memorial guest network, FMD and Webmail.

2. Workforce members using FMD to print when either on or off site must follow UMass Memorial Privacy and Information Security policies regarding physical security to prevent the printed material from being inappropriately disclosed.
3. 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.
4. Never save UMass Memorial 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, will be disconnected 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 or locked closet. When taken off site, laptops, mobile and data storage devices must be kept in the physicial 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 UMass Memorial records.
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 UMass Memorial email system may constitute privileged communications between UMass Memorial 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 UMass Memorial 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.

5. Confidential information may be transmitted via email within UMass Memorial with minimal risk.
6. When conducting UMass Memorial business, workforce members may only use their UMass Memorial email accounts. Use of a non-UMass Memorial email account, such as a Gmail, hotmail, or an account provided by another entity, is not permitted.
7. Occasional use of UMass Memorial email for personal reasons is permitted.
8. Text messages are not encrypted and therefore may not be used to transmit PHI.

G. Internet Use

1. The internet is to be used primarly in support of UMass Memorial 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. UMass Memorial utilizes an Internet content filtering tool which prohibits access to sites, including, but not limited, those in the categories of :

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

5. UMass Memorial 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 UMass Memorial 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 UMass Memorial 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.
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 UMass Memorial information.

3. All users will adhere to the proper procedures for accessing UMass Memorial's network, including the use of access tokens where indicated and strong passwords that are to be changed periodically. Refer to 05.06 Password Administration & Management Guidelines.

I. Prohibited Activities

Use of UMass Memorial 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 UMass Memorial 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 UMass Memorial 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 UMass Memorial and the third party.
4. Sending confidential information outside the UMass Memorial network without encryption.
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 UMass Memorial.
6. The intentional introduction of malicious programs onto UMass Memorial systems or networks (e.g. viruses, worms, Trojan horses, email bombs, etc.).
7. Making fraudulent offers of products, items or services originating from any UMass Memorial 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 UMass Memorial 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 UMass Memorial 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, UMass Memorial patients or employees to unauthorized parties outside UMass Memorial unless authorized by UMass Memorial management.
14. Any activity that is disruptive to the operation of UMass Memorial business.
15. Posting non-business-related messages to Usenet or Listserv servers.
16. Installing computer hardware or software on UMass Memorial electronic resources, including personal software and data without the approval of Information Services.
17. Downloading, file sharing, or storing UMass Memorial confidential information outside the UMass Memorial network except as authorized by the Chief Information Security Officer.
18. Using UMass Memorial 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 UMass Memorial email to an outside email account due to the potential negative impact on servers and to protect confidential information from being unsecurely sent over the internet.
22. Sending unsolicited email messages, including the sending of "junk mail" or other advertising materials (email spam).
23. Forging unanuthorized 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. Cyberbulling or posting/distributing discriminatory content is prohibited.
27. Using UMass Memorial confidential information for any unauthorized purpose or activity which violates the rights of privacy of UMass Memorial patients and workforce members. Refer to Policy 1421 Breach of Confidential Information.

J. Monitoring, Enforcement, Corrective Actions and Discipline

1. In order to assure the security of UMass Memorial confidential information and compliance with this policy, UMass Memorial actively monitors activity on its network and of its managed devices. UMass Memorial may monitor or review any data stored on managed devices at any time. UMass Memorial 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,

- Internet usage,
- Files, documents and faxes created, stored, deleted or distributed,
- Voice mail and messages,
- UMass Memorial confidential information , and
- Software, or applications owned or licensed to UMass Memorial.

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.
3. Workforce members must have no expectations of privacy in anything they create, store, send or receive on UMass Memorial electronic resources, on managed devices, or when using FMD or webmail.
4. Any workforce member using UMass Memorial electronic resources does so subject to UMass Memorial's rights to monitor such use and are advised that if monitoring reveals possible evidence of criminal activity, UMass Memorial may provide this information to law enforcement officials.
5. 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).
6. UMass Memorial reserves the right to revoke any user's access privileges at any time for violations of this policy, any other UMass Memorial policy, or conduct that disrupts the normal operation of UMass Memorial's information systems.
7. Violations of this policy could result in the permanent removal of ALL data, without notice, residing on managed devices and non-managed devices.
8. Violations of this policy can result in disciplinary action, up to and including immediate termination and/or legal action.

IV. Clinical/Departmental Procedure: N/A

V. Supplemental Materials: N/A

VI. References:

Policy 3000 Information Security Management
Policy 1421 Breach of Confidential Information
Policy 1428 Social Networking
Policy 4039 Discipline
Policy 4049 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.