LMH Health	**Title: Responsible Use Policy**
Number: 8110-002	
Document Category: Administrative	
Document Type: Administrative Policy	
Department/Committee Owner: IT - Administration	
Original Date: 01/01/2001	
Approval Date: 06/22/2020	
Approved By: President & CEO, Vice President & CIO	

1.0 Purpose

In support of its mission to provide high-quality health and wellness services to the community, Lawrence Memorial Hospital provides its workforce, which includes, employees, medical staff, contractors, volunteers and other authorized persons, use of LMH's Information Resources. "Information Resources" includes any and all LMH computers or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, use, or dissemination of data, including those that are individually controlled, shared, automated, manual, stand alone, or networked. Examples of Information Resources include, but are not limited to, electronic mail ("email") and other electronic messaging systems, Internet access software, Internet mail, file transfers, downloads, desktop software, software systems, voice communication tools, and other electronic media. The use of LMH's Information Resources is a privilege, not a right, and LMH expects all persons to use such resources in a responsible manner that complies with the Policy set forth below.

2.0 Scope

This policy applies to all members of the Lawrence Memorial Hospital workforce.

3.0 Policy

Electronic Communications

Email and other electronic messaging systems are an essential communication tool for LMH. Users are expected to use email and other electronic messaging systems in a respectful and appropriate way, using good judgment and common sense.

Use of email or other electronic messaging systems to engage in any communications in violation of LMH policies, including transmission of defamatory, obscene, pornographic, offensive, racist, sexist, threatening or harassing messages is prohibited. Users are not allowed to read, intercept, copy, use, or disclose email or other electronic messages directed to others without express authorization, unless such access is directly related to the User's job duties.

Email and other electronic messaging systems should not be used for any commercial purpose other than LMH business. Users are not allowed to use LMH's email or other electronic messaging systems for "spamming" or for pyramid or chain letters or other junk mail.

All Email and other electronic messaging communication should be done in a secure manner using approved security methods. Any use of email or other electronic messaging systems to transfer patient information must comply with LMH's HIPAA Privacy and Security policies. Unsecure email, texting, or other electronic communication of patient information is not authorized.

Internet Access

Access to the Internet is provided for LMH business purposes. Users are allowed limited personal use of the Internet, with certain restrictions intended to avoid unnecessary costs and burden to the Information Resources and to avoid inappropriate use. Use of sites that contain sexually explicit materials or sites dedicated to hate, violence, or gambling is strictly forbidden. This list is not exhaustive.

Ownership and Monitoring

LMH owns the rights to all data and files in any computer, network, or other Information Resources used at LMH and to all data and files sent or received using any company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property.

LMH reserves the right to monitor email and other electronic messages (including personal/private/instant messaging systems) and their content, as well as any and all use by Users of the Internet and of computer equipment used to create, view, or access email and Internet content. Users must be aware that the email and other electronic messages sent and received using LMH equipment or LMH-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by LMH officials at all times. Users' access of systems and files containing patient information are subject to audit in accordance with HIPAA Security standards.

LMH has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with LMH policies and state and federal laws. No User may access another User's computer, computer files, or electronic mail messages without prior authorization from the LMH Chief Information Officer or his/her designee.

All computers, laptops, and other computer hardware and devices issued by LMH are the property of LMH.

Users must return all data, software, hardware or devices including, but not limited to mobile phones, laptop computers, tablets, and other computing devices to the LMH Chief Information

Officer or his/her designee upon the User's termination of employment or other relationship with LMH.

Security
To prevent unauthorized access to LMH's Information Resources and to ensure that security updates can be applied to LMH's computers, it is recommended that LMH personnel logout from the network and restart their computers at the end of the workday. Users must lock logged-in computers that will be left unattended (Windows Key+L; to unlock, press Ctrl+Alt+Delete and then enter your password). Additionally, all portable and personal devices that access LMH systems and its data must be encrypted and password protected.

Users are prohibited from sharing their username and password to allow another person to log in to LMH's Information Resources under the User's credentials. Users are responsible for safeguarding their username and password to LMH's Information Resources from unauthorized disclosure.

The additional administrative, technical and physical safeguards contained in LMH's HIPAA Privacy and Security policies apply with respect to any LMH Information Resource that is used to access, use, or disclose electronic patient information.

Remote Network Access
Remote access to LMH's Information Resources is provided via web-based remote access or Virtual Private Network (VPN) access. Contact the LMH Information Technology Department for instructions on using remote access to LMH's Information Resources.

To minimize security risks to LMH's Information Resources, any device used for remote access to LMH should be encrypted and password protected, as well as have a suitable firewall, current anti-virus software or end-point protection with automatic updates, and current operating system security patches.

If a home wireless (WiFi) network is used to connect to LMH's Information Resources, Users must configure WPA2 or higher encryption in their router and or gateway to ensure a private and reliable connection and to avoid risk of unauthorized access to LMH's Information Resources.

The Information Technology Department Help Desk can provide education and recommendations for Firewall, Encryption, Anti-Virus, and WiFi Settings.

Software Licensing
LMH licenses the use of computer software from a variety of outside companies. It does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.

LMH does not allow or condone the unlicensed duplication of software, nor does it lend copies of the software it licenses for installation or use on other systems, including home computers. LMH also does not allow or condone the use or storage of unlicensed duplicated software. Anyone learning of any misuse of software or related documentation within the hospital should immediately notify the Chief Information Officer.

Non-Standard Software and Hardware
Users must obtain permission from the LMH Information Technology Department prior to connecting any non-LMH-standard peripherals (such as but not limited to, cameras, iPods, non-LMH issued cell phones, external storage devices such as USB memory sticks, and PDAs) to LMH computers or networks.
Because software transmitted by email or downloaded via the Internet frequently contains malicious code or conflicts with LMH's Information Resources, messages with software attachments and some downloads are blocked by LMH's anti-spam, antivirus, and end-point protection systems. In the event such an attachment is received, do not open, install, or use it, including items such as screen savers, games, cartoons, animated attachments, or program files of any type.

Compliance
LMH Information Technology Department provides oversight when activity is found that jeopardizes compliance to this policy.

4.0 Related Laws, Regulations, Polices, or Procedures

4.1 45 CFR §164.308(a)(3)(i) HIPAA Administrative Safeguards – Workforce Security
4.2 45 CFR §164.308(a)(5)(i) HIPAA Administrative Safeguards – Security Awareness and Training
4.3 IT SMP 12.4 End Point Protection Management
4.4 IT SMP 14.1 Workforce Security, Clearance, and Termination
4.5 IT SMP 15.1 Security Awareness and Training
4.6 IT SMP 16.1 Password Management
4.7 Corrective Action HRP-50

5.0 Definitions

5.1

6.0 Sanctions

All Associates are expected to perform in a manner consistent with LMH's Purpose, Beliefs, and Policies. When this does not occur, corrective action may result, up to and including termination.

7.0 Questions/Waivers

Questions regarding this policy should be directed to Vice President & CIO.

8.0 Document History

Rev	Date	Approved By	Comment
0	01/01/2001	Vice President & CIO	Creation of Original Document
1	09/01/2012	Vice President & CIO Vice President, Human Resources Administrative Council President & CEO	Minor Revisions
2	03/01/2016	Vice President & CIO Vice President, Human Resources Administrative Council President & CEO	Major Revisions
3	04/17/2018	Vice President & CIO President & CEO	Periodic Review
4	06/12/2019	Vice President & CIO President & CEO	Approved