Main Line Health, Inc. and Main Line Health, Inc. Subsidiaries		
Working Together to Serve the Community		
This policy applicable to:	X All Subsidiaries X All Hospitals X All Acute Care Hospitals	X BMRH X Mirmont Treatment Center

HUMAN RESOURCES POLICIES AND PROCEDURES

Policy Name: Communications Technology Usage

Policy Purpose: To ensure that all Authorized Users, (including, but not limited to, employees, medical staff, volunteers, on-site vendors, and consultants), are responsible, productive users of Main Line Health (MLH) communications technologies, including computers, telephones, electronic mail system, copy/fax multi-device machines, printers and all forms of Internet/Intranet access. Authorized Users must use MLH communications technologies appropriately to protect patient information and the organization's business initiatives, assets and trade secrets.

Policy Statement: Access to MLH communications technologies is provided to Authorized Users for the benefit of MLH. Brief and occasional personal use of MLH's communications technologies and/or of an Authorized User's personal communications technologies by the Authorized User is acceptable as long as this use is not excessive or inappropriate, does not interfere with or distract the Authorized User or any other Authorized User from their job responsibilities, is not offensive, a nuisance or injurious to patients, and does not result in expense to MLH. MLH management retains the right to revoke this personal use exception at any time, whether in individual cases as a result of misuse or policy violation, or as a change for one or more MLH operating divisions, or across all MLH organizations. MLH may block and/or monitor access to streaming audio and video sites.

- All MLH policies and procedures apply to Authorized Users' conduct on the Internet, especially, but not exclusively relating to: the intellectual property of MLH or that which may be licensed to it by its vendors; the confidentiality of its patient information, under HIPAA or otherwise; dissemination of MLH information; MLH's standards of conduct (including without limitation any anti-harassment policies or other policy or legal requirements with respect to harassing behavior); misuse of MLH's resources, and the privacy and security of MLH's information and data.

- Under absolutely no circumstance is any MLH property to be utilized to solicit, harass, or otherwise offend any person or entity, or for any other unlawful purpose, such as access to inappropriate, illegally distributed or otherwise unlawful material. Use of the Internet or other electronic media must not disrupt the operation of the MLH network or the networks of other users. It must not interfere with employee productivity. Misuse of MLH communications technologies and/or violation of any portion of this Communications Technology Usage policy are subject to Performance Management action up to and including termination of employment. MLH will comply with requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

I. Procedure

A. Prohibited/Unacceptable Use of Communications Technologies (includes, but not limited to):

1. Any form of peer-to-peer networking or FTP (File Transfer Protocol) downloading of software for business or personal reasons without express written permission from Main Line Health Information Technology
2. Unauthorized downloading or installing of any software. All software installs must be done through the IT Department
3. Inappropriate software copied onto MLH owned, leased or licensed computer systems (e.g., pornographic material, pirated software, discriminatory information, advertisements used for commercial enterprises)
4. Violating software licensing agreements and copyright laws. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("SPAM") that is unrelated to legitimate MLH business
5. Excessive or inappropriate use for private or personal business activities
6. Personal use of cell phones and electronic devices may be restricted to breaks and assigned areas.
7. Misrepresenting oneself or MLH
8. Violating the laws and regulations of the United States or any other nation with whom MLH does business or any state, city, province, or other local jurisdiction in any way
9. Engaging in unlawful or malicious activities
10. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or any other code or file designed to disrupt, disable, impair, or otherwise harm either MLH networks or systems, or those of any other individual or entity
11. Causing congestion, disruption, disablement, alteration or impairment of MLH networks or systems
12. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in work-related messages
13. Storing private/personal data files, including, but not limited to multimedia files (i.e. movies, music and pictures) on any MLH communications system
14. Using MLH equipment to maintain, organize or participate in non-work-related Weblogs ("blogs"), Web journals, "chat rooms", or multiple simultaneous private/personal instant messaging conversations unless approved by the MLH Communications Technology Committee
15. Using MLH communications systems to access social networking sites (such as Facebook, Twitter, YouTube, blogs, etc.) for purposes other than pre-approved work-related projects. Appropriate business use of social networking is addressed in the Social Media Policy
16. Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended
17. The use of personal cameras, cell phones and other similar devices, in any area of the hospital, to photograph or otherwise transmit images of patients, medical procedures, personnel, and/or hospital property/premises is prohibited. When patients are the subject of Photographing or Videotaping, prior proper written consent to use the patient's photograph or likeness must be obtained from the patient or the patient's authorized representative. The written consent shall include the circumstances of the use of the Photographing or Videotaping and should be taken only on a Main Line Health authorized device.
18. Protected health information (PHI) should not be sent in messages via the Main Line Health WebXchange paging system
19. Internal Audit and External Phishing Violations/Failures are subject to Performance Management action up to and including termination of employment.
20. Defeating or attempting to defeat security restrictions on MLH systems and applications, including, but not limited to, installing non-standard Web browsers
21. E-mail signatures and taglines must only reflect Main Line Health specific verbiage and references and should not include personal, religious, quotations, symbols or graphics

B. Ownership and Access of Telecommunications, Electronic Mail, Internet Access, and Computer Files

1. MLH owns the rights to all data and files in any telecommunications, computer, network, or other information systems that are the property of MLH or used by MLH employees for job performance. MLH also reserves the right to monitor electronic mail messages sent by MLH equipment (including personal/private instant messaging systems) and their content, as well as any and all use of MLH phones, Internet and MLH computer equipment used to create, view, or access e-mail and Internet content
2. All forms of electronic communications, including Internet access, instant messaging, electronic mail messages and telecommunications sent and received using MLH equipment are not private and are subject to viewing, filtering, blocking, downloading, inspection, release, and archiving by MLH at all times. The release of specific information is subject to applicable state and federal laws and MLH rules, policies (see HIPAA and Main Line Health Standards of Conduct policies), and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software
3. MLH 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 policy and state and federal laws, and to delete them without prior notification if they are unrelated to MLH business
4. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from Human Resources. Authorized Human Resources and Information Services and Legal Department personnel are exempt from this prohibition in order to perform administrative duties in accordance with MLH policy
5. Electronic mail messages received should not be altered without the sender's permission, nor should electronic mail be altered and sent to another user. Unauthorized attachments should not be placed on another individual's electronic mail message
6. Employees are individually liable for any and all damages incurred as a result of violating MLH privacy and security policies, copyrights and licensing agreements

Origination Date: September, 2006

Revision Date: August 2019; December 2017; November 2016; June, 2014; July, 2011

Last Review Date: August 2019; June, 2018; June, 2017; November, 2016; June, 2016; June, 2015; June, 2014; June, 2012; July, 2011; August, 2008