POLICY AND PROCEDURES MANUAL
LAKEWOOD HEALTH SYSTEM

SECTION: HIPAA
EFFECTIVE: January 2003 / April 2014
SUBJECT: Acceptable Usage and Agreement – Network, Remote Access and Email
REVIEWED: March 2021
SOURCE: HIPAA
REVISED: July 2009, May 2011, June 2019, March 2021
C TAG REF:

Purpose:

The purpose of this policy is to define standards for acceptable use when connecting to Lakewood Health System's network along with utilizing Lakewood Health System email. Email should not be overused or misused. These standards are designed to minimize the potential exposure to Lakewood Health System from damages, which may result from unauthorized use of Lakewood Health System resources. Damages include, but are not limited to, the loss of sensitive or company confidential data, intellectual property, damage to public image, and damage to critical Lakewood Health System protected health information systems.

Scope:

This policy applies to all Lakewood Health System employees, contractors, consultants, vendors, temporaries, agents, and others including all personnel affiliated with third parties utilizing Lakewood Health Systems network on location or via remote access. Remote access implementations that are covered by this policy include, but are not limited to, ISDN, DSL, VPN, SSH, Citrix, and cable modems. This policy also applies to anyone granted an email address by Lakewood Health System.

Policy:

Email

1. Lakewood Health System may access and monitor e-mail at any time for any reason without notice.
2. Lakewood Health System will archive all ingoing and outgoing emails. These archived emails may be accessed by Administration at any time when deemed necessary.
3. Accessing personal e-mail accounts (i.e., Yahoo, Hotmail, etc.) through Lakewood Health System's network is not allowed. If an exception is needed, this must be approved by O&P.
4. Auto-forwarding e-mail sent to LHS e-mail accounts to external accounts is prohibited without the HIPAA Security Officers prior approval.
5. Opening any attachments from a personal e-mail account is strictly prohibited.
6. System users should exercise extreme judgment and common sense when distributing messages.
7. Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing financial information, social security numbers, or other identifying numbers. Patient-related messages should be carefully guarded and protected, like any other written materials.
8. Email containing personal health information must be sent encrypted, i.e., using the "Send Secure" option, when sending to recipients outside of Lakewood Health System Failure to do so is considered a HIPAA violation and could result in disciplinary action. For more information around sending secure email messages, please reach out to IT for instructions on how to do so.
9. Never share your password to your account to allow others to access your email inbox.
10. You must also abide by copyright laws, ethics rules and other applicable laws.
11. Wagering, betting, or selling chances is prohibited
12. Sending chain letters, harassing, abusive, intimidating, discriminatory, racist, sexist, or other offensive emails is strictly prohibited.
13. The use of the system to solicit for any purpose without the consent of the VP of IT is strictly prohibited.
14. Attachment Guidelines for e-mail receivers
    a. If you do not know the sender, do not open the attachment.

   b. If the accompanying message is odd, do not open the attachment.
   c. If the subject line is questionable, delete the message without opening the attachment.
   d. If you have any questions around an email, please contact the IT Help Desk at 211 or by emailing helpdesk@lakewoodhealthsystem.com.

15. If you receive a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without permission, you must delete it immediately and not forward it. Chain-type messages and executable files should also be deleted and not forwarded because they cause overload on our system. Anyone engaging in the transmission of inappropriate e-mails, as determined by Lakewood Health System, will be subject to discipline, up to and including termination.
16. The Information Services Department will get signed policy agreements from all e-mail users, which will be filed in the employee's personnel file. After February 2019, all users of Lakewood Health System email will be required to have multi factor authentication in order to access their email messages outside of the Lakewood Health System network. Please refer to the Multi Factor Authentication policy accordingly.
17. By agreeing to this policy, you are also agreeing to information contained within the Cybersecurity Phishing Campaign Test Reporting and Corrective Action/Disciplinary Process policy.

Network

1. It is the responsibility of Lakewood Health System (LHS) employees, contractors, consultants, vendors, temporaries, agents, and others with access privileges to Lakewood Health System's corporate network to ensure that while connected locally or via remote access, their connection is securely protected. Only LHS owned and managed devices should be connected to the LHS internal (corporate) network. All other devices must connect to the LHS guest network or other external networks. If connected to the LHS guest network or other external networks and needing to access internal resources, users must utilize an encrypted connection such as Citrix or Cisco AnyConnect.
2. Only the person authorized and logged in under their user id may access LHS's network.
3. Please review the following policies for details of protecting information when accessing the corporate network. Copies of these policies can be obtained by contacting LHS Human Resources at any time.
   a. Workstation Security
   b. Establishing Access Controls – Electronic

Network Requirements

1. Network access must be strictly controlled. Control will be enforced via password authentication and also via Multi Factor Authentication in certain applications.
2. At no time should any Lakewood Health System employee, contractor, consultant, vendor, temporary, agent, and other worker provide their login password to anyone, not co-workers or family members. Doing so will subject the user to disciplinary action per the Disciplinary Action policy (A copy of this policy can be requested from LHS Human Resources at any time).
3. Lakewood Health System employees, contractors, consultants, vendors, temporaries, agents, and other workers with remote access privileges must ensure that their computer or workstation, which is remotely connected to Lakewood Health System's corporate network, is done so via an encrypted connection. LHS currently supports a Citrix remote access connection or Cisco AnyConnect VPN connection to ensure encryption. The HIPAA Security Officer must approve any exceptions to these type of connections.
4. VP of IT must approve non-standard hardware/software configurations, and the HIPAA Security Officer must approve security configurations for access to the network.
5. All devices that are connected to Lakewood Health System internal network via remote access technologies must use the most up-to-date anti-virus software. Anti-virus software definitions must be updated daily. Virus scans are to be completed regularly. LHS reserves the right to implement policies to deny connections to devices that don't have updated anti-virus software or definitions.
6. Personal equipment that is used to connect to LHS networks via an encrypted VPN (e.g. Cisco AnyConnect) must meet the requirements of LHS-owned equipment.

7. Wireless networks used to connect to LHS via remote access should have security encryption enabled at a minimum. LHS Information Technology will work with users to ensure that they are on an encrypted wireless network if need be.

Policy Enforcement:

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment. Any contractor, consultant, vendor, temporary, or agent found to have violated this policy will be subject to termination of contract and will be liable for damages. Damages include, but are not limited to, loss of Lakewood Health System protected Patient Health Information and damage to the reputation of Lakewood Health System.

Waiver of Privacy:

Lakewood Health System has the right, but not the duty, to monitor all aspects of its computer system, including, but not limited to, monitoring sites employees visit on the Internet, reviewing material downloaded or uploaded by employees, and reviewing email sent or received by employees. Employees waive any right to privacy in anything they create, store, send or receive on the system or the Internet.

DEPARTMENTAL APPROVAL:	2003/01
POLICY/PROCEDURE COMMITTEE APPROVAL:	2007/07

Access Desired:

□ LHS internal network

□ Remote access (Note: remote access is granted on a needs basis and must be approved by division director)

Reason remote access needed:

I have read and understand Lakewood Health System Acceptable Usage and Agreement Policy and agree to abide by it. I understand that violation of any above policies may result in termination of employment or termination of contract.

Signature: Date:

Printed Name: Phone:

Department: Position:

Company Name (if not an employee): Copy Similar User:

Company Address:

REQUIRED SIGNATURES:

Manager / HR Signature: ____

VP Signature: ____

VP of IT Signature: ________________________________

FOR INFORMATION SERVICES ONLY

Network access completed by:

Remote access completed by:

Date completed: