LakeCounty
Health Department and
Community Health Center

CORPORATE POLICY

SUBJECT: Electronic Communications	CATEGORY: Human Resources ORIGINAL DATE: November 7, 2001 REVIEWED DATE: November 29, 2017 REVISION DATE: April 30, 2025

I. POLICY:

This policy is intended to serve as a guide on the proper use of Lake County Health Department and Community Health Center (LCHD/CHC) electronic communication systems. This policy covers the use of all forms of electronic communications including but not limited to e-mail, voice mail, facsimile, external electronic bulletin boards, intranet, and the internet. Every employee is expected to read, understand and follow the provisions of this policy and will be held responsible for knowing its contents. Use of Lake County's electronic communication systems constitutes acceptance of this policy and its requirements.

II. SCOPE:

All LCHD/CHC full-time, part-time, and temporary employees, volunteers, contract, interns, and students.

III. PROCEDURE:

A. Acceptable use of Electronic Communications
   1. Work-Related use: Electronic communication tools should primarily be used for LCHD/CHC related activities, including patient care, administrative tasks and internal collaboration. Before using these systems for business or personal use, employees must understand that any information created, sent, received, accessed or stored in these systems will be the property of LCHD/CHC and will not be private. If employees are permitted to use electronic communication systems for non-work purposes, such use shall not violate any section of this policy or interfere with the employee's work performance.
   2. **Professional: Communications** must be professional, respectful and aligned with Lake County Employee Policies and Procedures Ordinance.
   3. **Appropriate Content: Ensure** that content shared via electronic communication is relevant, appropriate and does not violate patient privacy and confidentiality.

B. Prohibited Communications.
   1. Sharing, creating or downloading content that is discriminatory, harassing, illegal, sexually offensive, defamatory or interfering with the productivity of co-workers using LCHD/CHC electronic communication systems is strictly prohibited. Employees may not engage in any use which violates copyright or trademark laws.
   2. Employees are also prohibited from posting information, opinions, or comments to Internet discussion groups (for example: news groups, chat rooms, list servers or electronic bulletin boards) without prior authorization from the employee's supervisor. Employees in roles where the core job function include such postings are exempt from needing supervisor authorization for each post and are expected to follow guiding principles defined by their supervisor.

4. Under no circumstances may employees represent their own views as those of LCHD/CHC. Personal Health Information (PHI) must not be shared without proper authorization, in accordance with HIPAA and other relevant privacy laws. Employees shall not forward legally protected information from their LCHD/CHC email to a personal email account. Employees may send this content to the patient or to third parties, provided that we have obtained the necessary releases of information authorizing such sharing. Ensure Personally identifiable information (PII) or Protected Health Information (PHI) is encrypted when transmitting over the network. Please refer to the Email Encryption of Confidential Information Policy and the Data Transmission Policy for appropriate mechanisms to send this type of information when required. Personal information such as the home address, phone numbers and social security numbers of County employees should never be disclosed on the internet.
5. Employees must use their real names when sending email messages or other electronic communications. Employees may not misrepresent or conceal the identity of the real person responsible for electronic communication. Sending an email under a fictitious or false name is a violation of this policy. Electronic mail received shall not be altered without the sender's permission or changed and forwarded to another user. The exception to this would be if communication is being sent from a general email box.
6. The LCHD/CHC employees shall not access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's duties.
7. Employees must not maintain, organize or participate in non-work-related weblogs ("blog"), web journals, "chat rooms" or private/personal messaging during work hours or on company devices. This helps maintain the focus on work-related tasks and ensures the integrity and security of LCHD/CHC online presence.
8. Text messaging patient sensitive information, such as Protected Health Information (PHI), is prohibited. Text messaging PHI is generally not considered secure because it lacks the necessary security features like encryption, access control and audit trails required to protect sensitive health information, making it a potential violation of HIPAA regulations.

C. No Presumption of Privacy.
   1. LCHD/CHC electronic communication systems, including but not limited to email, voicemail, internet access and the intranet, are provided for business-related purposes. While we encourage responsible and professional use, employees should have no expectation of privacy when using these systems.
      Employees should always assume that any communications, whether business-related or personal, created, sent, received or stored on the Health Department 's electronic communication systems may be read by someone other than the intended recipient, including but not limited to review by a FOIA (Freedom of Information Act).
   2. Employees should also recognize that e-mail messages deleted from the system may still be retrieved from the computer's back-up system when requested by

authorized personnel. Consequently, messages that were previously deleted may be re-created, printed, or forwarded without the employee's knowledge.

D. Lake County's Right to Monitor Use.
   1. LCHD/CHC reserves the right to monitor, access and review any communication sent or received through these systems, for reasons including, but not limited to, confidentiality or security, legal compliance and performance management. These inspections will also be conducted when it is necessary to find important information that cannot be easily accessed through less intrusive methods.
   2. These inspections will also be conducted when it is necessary to locate substantive information that is not more readily available by less intrusive methods.
   3. Before providing access to stored electronic communications such as e-mail, written authorization or requests will be required from the Human Resources Director or designee, or the Compliance Officer.
   4. Access to employee internet history will be authorized in the same manner as other electronic communications. However, LCHD/CHC will regularly monitor and maintain a log of employees' internet history including the type of sites accessed, the name of the server, and the time of day the access occurred. Directors will have access to this log upon request.
   5. Information obtained through monitoring may be used as a basis for employee discipline or termination.

E. Televideo/Conference.
   1. Televideo tools may be used for routine follow-up visits, consultations and mental health assessments, when clinically appropriate.
   2. Only LCHD/CHC approved, HIPAA compliant software and communication platforms may be used for televideo or virtual consultations. Approved tools should be secure, encrypted, and comply with relevant privacy standards to ensure the confidentiality of patient information.
   3. All virtual consultations should take place in private settings to prevent unauthorized persons from overhearing or viewing the session.
   4. No session, consultation, or conference may be recorded unless the patient provides written consent.
   5. All patient-related data shared during televideo consultations must be treated as confidential and protected in compliance with HIPAA and other applicable privacy regulations.

F. Prohibited Activities.
   1. Employees may not upload, download, or otherwise transmit copyrighted, trademarked, or patented material, trade secrets, or confidential, private or proprietary information or materials without their Director's authorization. Employees may not upload, download or otherwise transmit any illegal information or materials. Employees may not use LCHD/CHC's electronic communication systems to gain unauthorized access to remote computers or other systems or to damage, alter, or disrupt such computers or systems in any

way, nor may employees use someone else's code or password or disclose anyone's code or password including their own without authorization from their Director. Please refer to the Acceptable Use of Information Systems Policy for a detailed understanding of the appropriate use of information technology devices.

2. It is a violation of this policy for employees to intentionally intercept, eavesdrop, record, or alter another person's Internet and e-mail messages. Employees may not enable unauthorized individuals to have access to or use LCHD/CHC's electronic communication systems, or otherwise permit any use which would jeopardize the security of the County's electronic communication systems.
3. Employees must use their real names when sending e-mail messages or other electronic communications and may not misrepresent, obscure or in any way attempt to subvert the information necessary to identify the real person responsible for the electronic communication. Sending an e-mail message under a fictitious or false name is a violation of this policy. Likewise, using another user's account or login ID constitutes a violation of this policy.

G. Communications Branding. To ensure visual and brand consistency across all print and online materials, employees are required to follow LCHD/CHC's Brand Guidelines posted on the employee Intranet site, HealthNet. These guidelines cover official messaging and treatment of such assets as LCHD/CHC's name, logo, colors, and typography.

H. Disclaimer of Liability for Use of the Internet. LCHD/CHC is not responsible for material viewed or downloaded by employees from the Internet. The Internet provides access to a significant amount of information, some of which contains offensive, sexually explicit or otherwise inappropriate. It is difficult to avoid contact with this material; therefore, users of the Internet do so at their own risk.

I. Duty to Not Waste Electronic Communications Resources. Employees should avoid wasting electronic communication resources or using them in a way that unfairly limits access for others. This includes actions like subscribing to unrelated list servers, mailing lists, spending excessive time on non-work-related websites, downloading large files for personal use, or sending mass emails. To ensure that company resources, including internet bandwidth, are used efficiently for work-related tasks, employees are prohibited from streaming non-work-related content (such as movies, TV shows, music, videos or podcast) during work hours, unless the content is directly related to work activities or has been approved by management.

J. E-mail Addresses. LCHD/CHC reserves the right to keep an employee's e-mail address active for a reasonable period following an employee's departure to ensure important business communications reach the County.

K. Record Retention. Generally, e-mail messages are usually temporary communications which are non-vital and may be deleted regularly. This is a rich source of information for cyber-attacks and emails considered sensitive with attachments should be saved to folders and then deleted immediately. However, if

the email contains important information, it may need to be kept according to the department's record retention policy. It is important to note that the Local Records Act, 50 ILCS 205/1 et seq., defines "public record" to include digitized electronic material. Therefore, for purposes of this Act, LCHD/CHC employees should treat e-mail messages and other electronic records in the same manner as if these messages had originated on paper. Employees should consult their supervisor or Director for guidance in determining what records are subject to retention. The Retention and Destruction of Protected Health Information Policy lists specific guidance on the data we are required to retain.

L. Freedom of Information Act (FOIA) Requests. LCHD/CHC designated FOIA Officers shall process FOIA requests consistent with guidance and requirements in the Act, 5 ILCS 140, as it pertains to the use of electronic systems to submit or respond to requests.

M. Violations.
   1. Violations of this policy may subject employees to disciplinary action beginning with the removal of privileges up to and including dismissal from employment and, if applicable, any criminal or civil penalties or other legal action. Refer to the HIPAA Sanctions for Privacy and Security Violations by Workforce Members Policy.
   2. Employees who observe violations of this policy are obligated to report those violations to their Director or to Human Resources.
   3. The Human Resources Director or Executive Director may authorize individuals, for investigative purposes, to engage in activities otherwise prohibited by this policy.

N. Policy Changes. LCHD/CHC reserves the right to change this policy at any time without notice. Nothing contained in this policy is intended to be or should be construed as an agreement and/or a contract, express or implied.

O. Definitions Applicable to this Policy.
   1. Electronic Mail (e-mail): Electronic mail may include non-interactive communication of text, data, image or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "mail," "facsimile," or "messaging" systems; or voice messages transmitted and stored for later retrieval from a computer system.
   2. Internet: A worldwide network of networks, connecting informational networks communicating through a common communications language, or "protocol."
   3. Intranet: An in-house web site that serves the employees of the enterprise. Although Intranet pages may link to the Internet, an Intranet is not a site accessed by the public.
   4. List Servers: An e-mail discussion group.

IV. REFERENCES:

Lake County Employee Policies and Procedures Ordinance
Local Records Act, 50 ILCS 205/1 et seq.

CORPORATE POLICY

Freedom of Information Act, 5 ILCS 140
Email Encryption of Confidential Information Policy
Data Transmission Policy
HIPAA Sanctions for Privacy and Security Violations by Workforce Members Policy
Retention and Destruction of Protected Health Information Policy
Acceptable Use of Information Systems Policy
Intrusion and Data Loss Prevention Policy

V. AUTHORS/REVIEWERS:
Designated Review Team, Corporate Policy and Procedure Committee, Executive Team, and Lake County Board of Health Personnel Committee.

VI. APPROVALS:
Lake County Board of Health President

Signature: _____ Date: _____