

**LOUISIANA STATE UNIVERSITY
HEALTH CARE SERVICES DIVISION**

POLICY NUMBER: 4511-21

CATEGORY: Human Resources

CONTENT: E-Mail Policy

APPLICABILITY: This policy applies to all persons employed by the LSU Health Care Services Division Headquarters (HCSDA) or the Lallie Kemp Medical Center (LKMC) either through direct hire or through contractual arrangement.

EFFECTIVE DATE: November 20, 1996
July 20, 2001
March 5, 2008

REVIEWED: January 4, 2010
June 13, 2011

REVISED: April 1, 2014

REVIEWED: February 6, 2015

REVIEWED: March 21, 2017

REVISED: June 9, 2017

REVISED: December 10, 2018

REVIEWED: November 25, 2019

REVIEWED: May 28, 2020

REVISED: March 31, 2021

INQUIRES TO: Human Resources Administration
LSU - Health Care Services Division
Post Office Box 91308
Baton Rouge, LA 70821-1308
(225) 354-4843 FAX (225) 354-4851

Note: Approval signatures/titles are on the last page

E-MAIL POLICY
LSU - HEALTH CARE SERVICES DIVISION

I. STATEMENT OF POLICY

It is the policy of the LSU Health Care Services Division (HCSD) to comply in all respects with the LSU System Information Security Policy (PM-36), the LSUHSC Enterprise Information Security Policy (EIS-100), LSU HCSD Information Security policy (7701), and the privacy and security protections mandated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Therefore, it is the policy of the HCSD to ensure that confidential information is protected by adequate safeguards when communicating via electronic mail (E-Mail), that E-Mail is used only for HCSD business purposes, proper email set up and etiquette is followed and the E-Mail users are aware that communications sent or received by HCSD employees may be monitored at the discretion of HCSD.

Note: Any reference herein to Health Care Services Division (HCSD) also applies and pertains to Lallie Kemp Medical Center (LKMC).

II. IMPLEMENTATION

This policy and subsequent revision to this policy shall become effective upon approval of the HCSD Chief Operations Officer (COO).

III. RESPONSIBILITIES

HCSD Executive Staff members and Lallie Kemp Hospital Administrator are responsible for assuring managers, supervisors, and employees within their organizational authority comply with the provisions and intent of this policy.

Each employee shall sign an acknowledgment form noting he or she has received a copy of this policy. This attestation may also be ascertained through the HCSD on-line training system. This acknowledgement shall become part of the employee’s human resources file and/or educational training record. (See ATTACHMENT #1)

IV. GENERAL PROVISIONS

- A. HCSD E-Mail systems are for use by all authorized employees of HCSD for the purpose of fulfilling their responsibilities and job duties. Only the HCSD E-Mail system shall be used to communicate official HCSD business. Public or personal E-Mail systems shall not be used to communicate official HCSD business.
- B. HCSD E-Mail should be considered as one of several methods of producing interdepartmental correspondence that may be reviewed at any level of the HCSD’s management. E-Mails are public record.
- C. HCSD E-Mail transmissions are subject to monitoring for waste, fraud, and/or abuse. Although electronic communications may be protected by a person’s confidential

password, privacy is not guaranteed.

- D. HCSD has a need and obligation to maintain efficient and effective communication amongst its employees. Email represents one communication tool provided by HCSD to this end. As such, all employees are responsible for checking, reading and responding to Email in a regular and timely manner.
- E. HCSD employees must use caution when clicking links or opening attachments in email. HCSD employees should only click links and open attachments when the email is from a known source and the contents of the email is expected from this known source. Email has become a major target for malicious content. The malicious content is often delivered as a web link within the body of the email and upon being clicked, opens a web browser to a website containing malicious content, which can infect HCSD electronic systems. A malicious web link can be any link in the email message, including, for example, the unsubscribe link in the email or any clickable email address in the email. Every clickable link in an email message could link to malicious content. The malicious content can also be delivered as an attachment of an email message.
- F. Highly confidential or sensitive communications SHALL NOT be communicated via E-Mail without authorization. Employees are expected to adhere to the mandates found in the LSU System Information Security Policy (PM-36), the LSUHSC Enterprise Information Security Policy (EIS-100), LSU HCSD Information Security policy (7701), and the privacy and security protections mandated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). This restriction includes but is not limited to Protected Health Information (PHI) and personal employee information in accordance with the following provisions:
 - 1. No email message or attachment shall contain a patient’s or group of patients’ PHI, such as, name, address, zip code, phone number, social security number, driver’s license number, health plan identifiers, age, date of birth, date of death, and medical conditions or diagnoses related to individually identifiable information about a patient or group of patients. The only exception would be to provide PHI in an email message or attachment, if directed to do so by the patient. Prior to providing PHI in an email message or attachment, the risk of sharing this information by email must be explained to the patient and the patient must accept the risk. The patient’s acceptance of this risk must be documented in the patient’s record.
 - 2. No email message or attachment shall contain the following information relating to an employee or group of employees of HCSD unless directly provided or requested by the employee in an email – social security number, driver’s license number, passport number, or provider credentialing identifiers such as medical license number, national provider identifier, state or federal (DEA) controlled substance license number.
 - 3. No email message or attachment shall contain the following information relating to an employee or group of employees, or patient or groups of

patients, of HCSD unless directly provided or requested by the employee or patient – (a) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account, (b) biometric data, defined as data generated by automatic measurements of an individual’s biological characteristics, such as finger prints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual’s identity when the individual accesses a system or account.

4. When required for business purposes, only the official LSU-HCSD E-Mail system shall be used to communicate information about employees. Personal or public E-Mail systems shall never be used to communicate employee information (such as Google mail, Yahoo mail, E-Mail provided by a home internet service provider). E-Mail communication of employee information shall be restricted to only that information necessary for proper identification of the employee, shall never contain confidential information and shall never contain the information described in section F.2 or F.3 above. This restriction applies to the content in the body of the E-Mail message and the content of any attachments.

5. It is understood that electronic communication of patient and employee information is sometimes essential to support efficient clinical and business processes. In an effort to protect patient PHI and confidential employee information, the following options may be used when sending patient PHI or confidential employee information:

- a. Use the LSU HCSD secure file transfer system, LSU Health FileS:
 - 1) Each HCSD facility is responsible for making available and providing training for employees on the use of secure file transfer of this information.
 - 2) The Information Technology Department can assist employees with the current available methods of secure file transfer.
- b. If both the sending and receiving employees have access to the electronic health record, Epic, Epic In-Basket messaging can be used to securely send information.
- c. Use a secure E-Mail system or secure portal of a third party vendor, to securely send the patient PHI or employee information.

G. Bulk emailing of information can be selectively used for business related communications but must be approved at a level appropriate to the scope and content of the information.

H. Every staff member has a responsibility to use department authorized E-Mail access in an effective, ethical, lawful and productive manner.

- I. Employees are accountable for the content of their files and messages.
- J. E-Mail access shall not be used for accessing, viewing, transmitting, receiving, retrieving, printing, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or sexually explicit.
- K. Employees shall not transmit abusive, profane or offensive language through the HCSD E-mail system. Harassment of any kind is prohibited.
- L. Employees shall not transmit messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference.
- M. Employees shall not initiate or forward emails containing pornographic or sexually explicit information.
- N. Employees shall not use email to access links that transmit streaming audio or video except where required to carry out job duties.
- O. Employees shall not use email for personal monetary gain or commercial purposes not directly related to HCSD business or for functions that are not related to one's job.
- P. Employees shall not use the HCSD email system to solicit others for commercial ventures, religious or political causes or other non-job related solicitations.
- Q. Employees shall not obtain or attempt to access the files or electronic mail of others unless authorized by the owner or as required for legitimate business need, security issues, or investigative purposes. Disclosure of any information obtained must abide by existing policy, laws, and regulations.
- R. Employees shall not construct a false communication that appears to be from someone else.
- S. Employees shall not send, forward, or reply to E-mail chain letters.
- T. Employees shall not send copies of documents or include the work of others that are in violation of copyright law.
- U. When employees are unable to respond to email in a timely manner due to travel, illness or leave, they shall post an out-of-office reply message noting the anticipated date of return, and will review and respond as necessary as soon as possible upon their return.
- V. Use of non-standard backgrounds and graphics in email transmissions is prohibited.

V. EMAIL STANDARD SET UP AND ETIQUETTE

- A. TO Field: Employees shall use the “To” field to send email only to those employees who the sender intends to have read the email message in detail and/or reply to the message. Employees shall use group email judiciously. Before sending emails using group distributions, employees shall make sure every recipient in a group will see pertinence in receiving the email.
- B. Reply to All Field: Employees shall make sure every recipient in the original email is in need of the response before using this field.
- C. Subject Field: Employees shall use the “subject” field to indicate the content and purpose for the email.
- D. CC Field: Employees shall make sure every recipient in the “cc” line will see pertinence or find value in receiving the email before it is sent.
- E. BCC Field: Employees shall use this field judiciously.
- F. Font: Standard font size of 10 to 14 shall be used. It is acceptable to use the default font and size installed with the Outlook Desktop client.
 - 1. Employees shall use a basic font when sending or replying to emails, such as Arial, Courier, Tahoma, Calibri, Times New Roman.
 - 2. Employees shall not use all CAPS in the body of an email as it is perceived as yelling.
 - 3. Use of larger or smaller, bolded or colored fonts for routine email communication is prohibited. The use of special fonts and colors to support specific content may be used.
- G. Signature Block: Employees shall use the signature block on external email communications. Signature blocks shall not contain graphics, logos, jumping, flashing or colored emoticons. Signature blocks shall be in the same standard font and size as the email. The Signature Block shall contain the following:
 - 1. Name
 - 2. Title
 - 3. Office/Hospital/ Department
 - 4. Phone #
 - 5. Email address
- H. Background/Graphics and Emoticons: Employees shall not use background graphics and/or emoticons in any email originating from the employees email account. The following are specifically prohibited:
 - 1. Decorative backgrounds
 - 2. Signature block graphics, logos, etc.

3. Jumping, flashing or colored emoticons such as seasonal graphics, smiley faces or university inspired graphics and logos.
- I. Timely Response: Employees shall respond to emails in a timely manner. Employees are expected to check email on a regular basis and respond in a timely manner, usually within two (2) business days.
 - J. Out of Office Reply Message: Employees who are out of the office either for personal or business matters and are unable to access email on a regular basis, shall place an out of office message on their email account. The message shall state the duration that they will be unable to access email and an alternate contact name, email address or phone number.
 - K. Confidentiality Statement: You may also include a confidentiality statement when transmitting sensitive information.

VI. ENFORCEMENT/VIOLATIONS

Failure to adhere to the intent of this policy may result in disciplinary action up to and including dismissal.

ATTACHMENT #1

E-MAIL POLICY

RECEIPT ACKNOWLEDGMENT

NOTE: If you are completing the review of the Administrative Guidelines as a lesson assignment through WILMA, you DO NOT need to print and sign. You will complete an attestation at the end of the WILMA lesson designated as the Test.

I received a copy of the Health Care Services Division E-Mail Policy. I agree to comply with the policy, procedures and guidelines as outlined in this policy.

I understand that violation of this policy may result in disciplinary action up to and including termination.

Employee's Name: _____
(Please Print)

Employee's Signature: _____

Date: _____

Document Metadata

Document Name: 4511-21 - Email.docx
Policy Number: 4511
Original Location: /LSU Health/HCSO/4500 - Human Resources
Created on: 11/20/1996
Published on: 04/14/2021
Last Review on: 04/14/2021
Next Review on: 04/14/2022
Effective on: 03/07/2019
Creator: Kees, James "Mickey"
HCSO Chief Information Officer
Committee / Policy Team: Main Policy Team
Owner/SME: Townsend, Kathy
HCSO Human Resources Director
Manager: Townsend, Kathy
HCSO Human Resources Director
Author(s): Wicker, Claire M.
PROJECT COORDINATOR
Approver(s): Townsend, Kathy
HCSO Human Resources Director
Buie, Lanette
Chief Operations Officer
Publisher: Wicker, Claire M.
PROJECT COORDINATOR

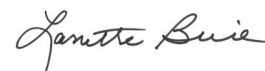
Summary of Changes/Updates:

No PHI in email.

Digital Signatures:

Currently Signed

Approver:
Buie, Lanette
Chief Operations Officer



04/14/2021

Approver:
Townsend, Kathy
HCSO Human Resources Director



04/14/2021