OCHSNER CLINICAL SCHOOL POLICY	Policy #: OCS 15329-2 (Related OMC Policy – 15329-2
Title: Email Access and Use	Effective Date: 1/1/10

POLICY

***Ochsner Clinical School Students will adhere to all institution policies and guidelines for email access and use. Institution Policy # 15329-2 follows. "Student" can be substituted for "employee" in the institutional policy.**

Ochsner Clinic Foundation's email system is to be used for business communications as described in this policy. OCF management reserves the right to inspect, monitor, record or delete any communications. While only authorized personnel will take these actions when circumstances warrant, employees should not have any privacy expectations in their email communications. Novell's Groupwise is the Ochsner Clinic Foundation (OCF) standard email and calendar/scheduling system.

PROCEDURES

I. The OCF email system is a communications system. The purpose of the email system is to faclitate business communications. It is not intended to replace formal business communication which should be transmitted by letters or other documents, to replace all telephone communications, or to be a vehicle for non-business communications.

II. Email messages may be transmitted internally or to recipients outside the OCF network using the Internet. The OCF email system can be accessed remotely from any properly equipped computer using the Internet or OCF's remote access system.

III. The data that accompanies an email transaction can vary from a brief message to a large attached file. Without concern for size, storage, archiving and management of data generated, performance of the email system becomes unpredictable and data security and integrity may be compromised. Accordingly, Groupwise content is retained for a limited time and attachments are subject to restriction.

IV. In addition to email, The Novell Groupwise system offers scheduling functions and provides facilities for recording notes or tasks.

V. Mailboxes will be assigned to OCS Students as appropriate. Each email user is given a "User ID" and is responsible for creating a unique password to prevent unauthorized access.

VI. It is the responsibility of each user to guard the confidentiality of his or her password in accordance with the Confidential Information Access-Employee Agreement.

VII. Mail messages will be deleted from the “In Box” and placed in the “Trash Bin” 60 days after receipt. Mail messages will be deleted from the Trash Bin 7 days after they are placed there.

VIII. Appointments, Tasks, and Notes will be placed in the Trash bin 60 days after entered. Appointments, Tasks and Notes will be deleted from the Trash Bin 7 days after they are placed there.

IX. Once deleted from the Trash Bin, items are generally unrecoverable.

X. Users are responsible for manually archiving or printing items they wish to retain for longer periods of time.

XI. Files attached to an email message should be no larger than 2MB. Files larger than 2MB will be deleted the next business day after they are sent. The preferred method for sharing large files is to place them on a file server drive.

XII. Unless special arrangements are made with the approval of the Chief Information Officer, mailboxes will be deleted immediately upon termination of employment with OCF. All items in a deleted mailbox will become unrecoverable.

XIII. Any item sent, received, or stored through the email system is the property of OCF and may be audited by management at any time. Until items have been deleted, either by the user emptying the Trash Bin or by the time delete process, they are recoverable and legally discoverable. It may be possible to recover some previously deleted message from the mail server’s disc storage system. Bearing this in mind, email messages should never include compromising or embarrassing content. The systems and communications may be subject to subpoena or other legal process. Employees should not communicate anything in email that they would not want read by anyone other than the addressed recipients.

XIV. Patient specific information must never be sent via the internet to a non-Ochsner address without encryption provided by Information Services.

XV. Managers are responsible for verifying that employees do not misuse OCF Internet email resources.

Examples of misuse include but are not limited to:

- Any activity that is unprofessional, unethical or illegal
- Harassment or defamation of other employees or third parties
- The unauthorized distribution of copyrighted materials
- Communication of any Ochsner confidential information without proper authorization
- Actions to further any non-business activity
- Usage beyond occasional non-business use.

XVI. The email communication system may not be used in any way that may be disruptive, offensive to others, or harmful to morale. Anyone violating this policy will be subject to corrective action up to and including termination of employment.

FORMS: Information Service Access/ID Request
Former AOMF Policy #: 8480-1-7
Former OC Policy #: 1300.4, OCF 8480-2

APPROVED BY:
Lynn R. Witherspoon, M.D., Vice President, Chief Information Officer
Warner L. Thomas, President, Chief Operating Officer

APPROVALS

SIGNATURES:

Professor William W. Pinsky
Head, Ochsner Clinical School
Executive Vice President /Chief Academic Officer

Ochsner Health System

Policy Number	OHS.IS.014
Date of Issue	December 2010
Date of Last Review	
Date of Last Revision	
Policy Owner(s)	Information Services Corporate Integrity

Email Acceptable Use

A. Purpose

The purpose of this Policy is to prevent misuse of Ochsner's Electronic Mail systems (E-mail).

B. Scope

Employees, contractors, part-time and temporary workers and those employed by others to perform work on Ochsner premises or who have been granted access to and use of Ochsner electronic mail resources are covered by this Policy and must comply with associated standards and procedures.

C. Policy Statements

1.0 Use of Ochsner electronic mail resources must not be illegal, must not constitute or be perceived as a conflict of company interest, must not violate company policies and standards and must not interfere with normal business activities and operations.

D. Standards and Roles & Responsibilities

Business Use

1.1 Ochsner's electronic mail (e-mail) resources are provided primarily for official and authorized Ochsner business use and to support patient care, clinical research and business operations.

1.2 The use of Ochsner electronic mail resources shall be in accordance with applicable laws and regulations.

1.3 Users shall be accountable for all electronic mail activity associated with their account(s).

1.4 Users are responsible for creating an appropriate password to prevent unauthorized access in accordance with the Access Control Policy.

1.5 All electronic mail resources and all messages created, received, processed, transmitted and/or stored on Ochsner resources are Ochsner's information assets and property.

1.6 Electronic mail messages and attachments containing Ochsner Electronic Protected Health Information (ePHI) and/or other sensitive/confidential data must be appropriately encrypted according to the Data Encryption Policy. Questions regarding confidentiality and encryption must be referred to Information Services' Information Security Services.

1.7 Public e-mail services or providers (such as Yahoo, Hotmail, Google, etc) shall not be used for the transmission of electronic mail messages or attachments containing ePHI and/or other sensitive/confidential information.

Email Acceptable Use

Improper Use

1.8 Ochsner electronic mail (e-mail) resources must not be used to forward chain letters, personal solicitations, unconfirmed virus warnings and/or hoaxes or support other such "re-mailing" (setting off a sudden heightened volume). Users must not respond to chain mail, or other software or features that automatically forward electronic mail messages to other email addresses.

1.9 Users must not alter the electronic mail software security settings applied by the Information Services Division.

1.10 Ochsner electronic mail resources must not be used to download, create, transmit or store objectionable or illegal material, images or content.

1.11 Users must not allow others to access electronic mail resources using their account. This does not include the use of GroupWise Proxy to manage another's Mailbox and Calendar. GroupWise Proxy lets you perform various actions such as reading, accepting, and declining items on behalf of another user, within the restrictions the other user sets.

1.12 Electronic mail messages over sixty (60) days in age are subject to deletion.

Right to Monitor

1.13 Users must not have expectations of privacy when using Ochsner assets to send or receive email messages.

1.14 Ochsner has the legal right to monitor and review all activities, messages and attachments using company electronic mail resources at any time.

1.15 Ochsner reserves the right to archive electronic mail resources in response to legal and/or e-discovery purposes without prior notice to the user.

1.16 Ochsner reserves the right to disclose the nature and content of e-mail messages and activities to law enforcement officials or other third parties without prior notice to the User.

Storage Capacity

1.17 Users shall delete unnecessary electronic mail messages to avoid excessive storage requirements on the Company's electronic mail servers.

1.18 Electronic mail messages are maintained on the mail server for sixty (60) days from receipt or submission.

1.19 Electronic mail messages over sixty (60) days in age are subject to deletion.

1.20 Electronic mail messages deleted by the user or placed in the "Trash Bin" are subject to deletion after seven (7) days.

Email Acceptable Use

1.21 Electronic mail messages over sixty (60) days in age or seven (7) days in the trash bin are subject to deletion

1.22 Electronic mail messages over sixty (60) days in age or seven (7) days in the Trash Bin are generally unrecoverable.

E. Enforcement and Exceptions

1.0 Requests for exceptions to the E-mail Acceptable Use Policy must be submitted in writing to the Chief Information Officer, CIO, and the Vice President of Corporate Integrity and must

1.1 Describe the reason for requesting an exception.

1.2 Describe the specific impact on workflow process or patient care if request is denied

1.3 Describe any system limitations causing compliance issues with this Policy along with any future plans to address.

2.0 Requests for exceptions will be answered in writing within 30 days of receipt of the request, approving, denying, or requesting additional information.

3.0 Failure to comply with the Email Acceptable Use Policy may result in corrective action in accordance with HR Policy 154020-500.2 Corrective Action Policy and/or termination of contract.

F. Definitions

1. Electronic Protected Health Information - (ePHI) under HIPAA means any electronic health information that identifies an individual.
2. Information Assets - Hardware or software that creates, receives, stores or transmits electronic data used for patient care, clinical research or in support of Ochsner business processes; including all data maintained or accessed through systems owned or administered by or on the behalf of Ochsner.
3. Internet resources Refers to the systems, networks, equipment, software and processes that provide access to and/or use of the internet including accessing, downloading, transmitting or storing data and information as well as the operation of software products and tools.
4. Objectionable - Refers to anything that could be reasonably considered to be obscene, indecent, harassing, offensive or any other uses that would reflect adversely on the Company including but not limited to comments or images that would offend, harass or threaten someone on the basis of his or her race, color, religion, national origin, gender, sexual preference or political beliefs.

Email Acceptable Use

5. Ochsner: Ochsner Health System and its members, affiliates and subsidiaries, existing now and hereafter created.
6. Personal Protected Information - means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:
7. (i) Social security number.
8. (ii) Driver's license number.
9. (iii) Account number, credit or debit card number
10. Personal information does not include publicly available information
11. Sensitive/Confidential data - is the classification designated for company information assets that create, receive, store, or transmit electronic protected health information (ePHI) and/or personal/sensitive information assets that if disclosed could be used to cause hardship, embarrassment or harm to Ochsner patients, employees or other customers. This classification includes Personal Protected Information.

G. Internal References

[This section intentionally left blank]

H. External References

[This section intentionally left blank]

I. Approved

Patrick Quinlan, M.D., Chief Executive Officer
Warner Thomas, President and Chief Operating Officer
Chris Belmont, Chief Information Officer

J. Policy History

15329-2 Email Access & Use