HIPAA Policy 5123
Electronic Communication of Health Related Information (Email, Voice Mail and other Electronic Messaging Systems)

Responsible Office	Office of the Provost	**Effective Date**	04/20/05
Responsible Official	University Chief Information Officer	**Last Revision**	3/8/16

Scope

This policy applies to the University's Covered Components and those working on behalf of the covered components, designated as such for purposes of complying with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996. The Covered Components are: (1) the Group Health Plan Component; and (2) the Covered Health Care Component, which includes the School of Nursing, the Department of Psychology clinics, Yale Health and the School of Medicine (except the School of Public Health and the Departments of Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, Pharmacology, and WM Keck Biotechnology Resources Laboratory).

This policy establishes standards for the electronic transmission of Protected Health Information ("PHI") and the controls that the Yale covered components will employ to protect the security and privacy of electronic PHI. This policy applies to email, instant messaging, voice mail, file transfer, and any other technology that transmits health information electronically.

Policy Statement

PHI that is to be transmitted electronically shall be transmitted in a manner that protects it against unauthorized access and ensures its integrity. To accommodate both the need to protect the PHI and the need for efficient communication of PHI in support of patient care, PHI may be transmitted electronically only when the use or disclosure is permitted in accordance with HIPAA policy 5031 "Authorization Requirements for Use and Disclosure of Protected Health Information and Identity Verification" and when the limited circumstances described herein are met. When the circumstances allow electronic transmission of PHI, reasonable and appropriate security measures shall be implemented.

Reason for the Policy

Compliance with HIPAA and related regulations.

Definitions

An **Electronic Message** is any message created, sent, forwarded, replied to, transmitted, stored, copied, downloaded, displayed, viewed, or read by means of telecommunications networks or computer systems. This definition applies equally to the contents of such messages; transactional information associated with such messages, such as headers, summaries, addresses, and addressees; and attachments (text, audio, video). This Policy applies only to Electronic Messages in their electronic form. The Policy does not apply to printed copies of Electronic Messages.

An **Electronic Messaging System** is any messaging system that depends on electronic facilities to create, send, forward, reply to, transmit, store, copy, download, display, view, or read Electronic Messages, including services such as email, text messaging, instant messaging, social networking, blogging, electronic bulletin boards, listservs, and newsgroups.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning to the data without the use of a confidential process or key.

A **Personal Representative** is someone with the legal authority to act on behalf of an incompetent adult patient, a minor patient, or a deceased patient or the patient's estate in making health care decisions or in exercising the patient's rights related to the individual's PHI.

Yale Personnel are faculty, staff, trainees, and students who work or train in Yale's HIPAA Covered Components.

Please also refer to the Master Glossary of HIPAA Security Terms in the Definitions section of Policy 5100 "Electronic Protected Health Information Security Compliance."

Policy Sections

5123.1 Reasonable and appropriate security measures for all Electronic Messages containing PHI

Yale Personnel must comply with the following security measures whenever PHI is included in an Electronic Message:

A. The use or disclosure of the PHI must be permitted by Policy 5031 "Authorization Requirements for Use and Disclosure of Protected Health Information and Identity Verification." (See "Related Information" below.)

B. Electronic Messages containing PHI may not be sent or received except with a device that has been secured in compliance with Yale's HIPAA security policies and procedures.

C. PHI must be limited to the minimum information necessary for the permitted purpose. (See Policy 5037 "Minimum Necessary Uses, Disclosures and Requests" under "Related Information" below.)

D. Highly sensitive PHI (for example, mental health, substance abuse, or HIV information) should be transmitted by Electronic Message only in exceptional circumstances.

E. Yale personnel must use a yale.edu email account to send and receive PHI, and they may not use any other email accounts (for example, Google or Yahoo accounts) for that purpose. A yale.edu email account that may send or receive PHI may never be set to auto-forward messages to a non-Yale account.

F. PHI may only be sent by email after the recipient's address has been carefully verified (for example, from a directory or a previous email) and entered correctly.

G. Electronic Messages containing PHI must include a privacy statement notifying the recipient of the insecurity of electronic messaging and providing a contact to whom a recipient can report a misdirected message. (See sample statements in the "Email Notice" section of "Guidance on the Use of Email Containing PHI" under "Related Information" below.)

H. PHI may never be sent through an Instant Messaging program not approved by the University for PHI.

If an Electronic Message is encrypted with an approved encryption program, then these measures are the only requirements that Yale imposes on the communication. If an Electronic Message is not encrypted with an approved program, then the communication must meet the additional requirements imposed by Section 5123.2, 5123.3, or 5123.4 below.

5123.2 Unencrypted Electronic Messages within and between Yale Electronic Messaging Systems and Yale New Haven Health System Electronic Messaging Systems

Yale Personnel may exchange Electronic Messages containing PHI among themselves and with Yale New Haven Health System ("YNHHS") personnel so long as (i) the security measures set out in Section 5123.1 are followed; and (ii) the Electronic Message remains wholly on Yale- or YNHHS-managed Electronic Messaging Systems and the connection to those systems are secured. (See Policy 1610 "Systems and Network Security" under "Related Information" below.) For example, e-mail messages between or among yale.edu and ynhh.org addresses are permitted under this Policy.

5123.3 Unencrypted Electronic Messages between Yale Personnel and external treatment providers or research collaborators

If the security measures set out in Section 5123.1 are followed, Electronic Messages containing PHI may be exchanged between Yale Personnel and external treatment providers or research collaborators in either of the following circumstances:

A. The Electronic Message (i) contains information urgently needed for patient care; and (ii) the patient identifiers are limited to name, date of birth, medical record number, or phone number, as needed.

B. The Electronic Message (i) is needed in a timely manner for the benefit of the patient or research subject; (ii) contains no highly sensitive PHI (for example, mental health, substance abuse, or HIV-related information); and (iii) contains none of the following direct identifiers: name, street address, Social Security number, date of birth, age if over 89, phone number, fax number, or patient email address. (Less direct identifiers such as medical record number or initials (for example, "Mr. S") may be included.)

5123.4 Unencrypted Electronic Messages between Yale Personnel and patients or research subjects

If the security measures set out in Section 5123.1 are followed, Electronic Messages containing PHI may be exchanged between Yale Personnel and a patient, a research subject, or a Personal Representative if, other options having been explained, (i) the patient, research subject, or Personal Representative has consented to the use of Electronic Messaging by completing a Consent for Email and/or Text Message Communication form; or (ii) after having been advised regarding the risks inherent in Electronic Messaging, the patient, research subject, or Personal Representative has provided oral consent and the oral consent has been noted in the individual's record. If oral consent is obtained, the required warning and request for consent shall be substantially similar to the following:

> Email and text messaging are not completely secure means of communication because these messages can be addressed to the wrong person or accessed improperly while in storage or during transmission. Knowing that there is this risk, do you want us to send information to you by email and/or text message?

5123.5 Misdirected Electronic Messages

Misdirected Electronic Messages must be documented in the Accounting for Disclosures log. (See Procedure 5003 "Accounting for Disclosures" policy under "Related Information" below.) Misdirected Electronic Messages may also be subject to reporting requirements as described in Policy 5005 "Reporting Incidents Involving the Security or Privacy of Protected Health Information: Breach Notification." (See "Related Information" below.)

5123.6 Use of Voice Mail for communication of PHI

If any PHI might be left on an individual's University or smartphone voice mail, that individual may not use the default password and must select a strong password. For guidance on the creation of a strong password see: http://dev.hipaa.yale.edu/guide-1610-gd01-selecting-good-passwords

Special Situations/Exceptions

Units of the Covered Components (for example, Yale Health) may establish practices and procedures that apply specifically to that unit provided that the practice or procedure is consistent with University policy and requires equal or greater security for PHI.

Related Information

Policy 1610: Systems and Network Security
Policy 1607: Yale University Information Technology Appropriate Use Policy on encryption: see ITAUP (section IV-F)
Procedure 1607PR1: Endorsed Encryption Implementation
Procedure 5111 PR.2: Safeguards for Computing Device Display Screens
Procedure 5003: Accounting for Disclosures
Policy 5005: Reporting Incidents Involving the Security or Privacy of Protected Health Information: Breach Notification.
Policy 5031: Authorization Requirements for Use and Disclosure of Protected Health Information and Identity Verification.
Policy 5037: Minimum Necessary Uses, Disclosures, and Requests
Policy 5039: Disclosure of De-identified Information and of Limited Data Sets
Please also refer to the comprehensive summary of HIPAA Security **Related Information** provided within Policy 5100 Electronic Protected Health Information Security Compliance.

Forms and Exhibits

5123 EX.A: Guidance on the Use of Email Containing PHI, including standard email signature language and related email managed for HIPAA.
Please also refer to the comprehensive summary of HIPAA Security **Forms and Exhibits** provided within Policy 5100 Electronic Protected Health Information Security Compliance.
5123 EX B. Informed Patient Consent for Electronic Messaging.

Procedures

Procedure 5123 PR.1 - Communication of PHI via Electronic Messaging

Contacts

Please refer to the comprehensive summary of HIPAA Security **Contacts** provided within Policy 5100 Electronic Protected Health Information Security Compliance.

Roles and Responsibilities

Please refer to the comprehensive summary of HIPAA Security **Roles and Responsibilities** provided within Policy 5100 Electronic Protected Health Information Security Compliance.

Revision History

Revised November 2010, technical correction March 2014, revised to accommodate email reminders via email March 2015, February 2016 revised per OCR guidance on individual's right to access PHI.