

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

<b>Responsible Office</b>	Office of the Provost	<b>Effective Date</b>	04/20/05
<b>Responsible Official</b>	University Chief Information Officer	<b>Last Revision</b>	04/20/05

<b>Policy Sections.....</b>	<b>2</b>
5123.1 Reasonable and Appropriate Security Measures .....	2
5123.2 Communications between Yale Electronic Messaging Systems and Yale New Haven Health System Electronic Messaging Systems .....	2
5123.3 Electronic messaging between Yale personnel and external treatment providers .....	3
5123.4 Electronic messaging between Yale personnel and patients .....	3
5123.5 Electronic messaging between Yale personnel and non-Yale individuals, research subjects or organizations .....	3
5123.6 Use of the Yale University Voice Mail for communication of protected health information .....	3

**Scope**

This policy applies to the University's Covered Components, designated as such for purposes of complying with the privacy and security 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, comprised of the School of Medicine, School of Nursing, Department of Psychology clinics and Yale University Health Services.

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

**Policy Statement**

To protect against unauthorized access and to maintain the integrity of the ePHI, reasonable and appropriate security measures shall be implemented when Protected Health Information (PHI) is transmitted electronically.

**Reason for the Policy**

Compliance with the 1996 Health Insurance Portability and Accountability Act.

**Definitions**

An **Electronic Message** is any or several electronic records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic messaging systems or services. This definition of electronic messages applies equally to the contents of such records and to transactional information associated with such messages, such as headers, summaries, addresses, and addressees. 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, hold, copy, download, display, view, read, or print messages for purposes of

communication across computer networks or systems between or among individuals or groups, that is either explicitly denoted as a system for electronic messaging or is implicitly used for such purposes, including services such as electronic bulletin boards, listservs, and newsgroups.

**Electronic Protected Health Information (ePHI)** is PHI in electronic form.

**Encryption** is the translation of data into a unintelligible condition based on a secret code. For all practical purposes, using current technology, the original data can only be restored by provision of that secret code (called Decryption).

**Insecure Electronic Messaging** is the transmission of electronic messages via a system which cannot protect those messages using encryption from when they enter the messaging system until delivered to the intended recipient.

**Secure Electronic Messaging** is the transmission of electronic messages via a system which has the capability of securely encrypting the messages from point of entry into the messaging system until delivered to the intended recipient in such a way that only that intended recipient can decrypt them. Some electronic messaging systems can send both secure and insecure electronic messages; messages sent via such a system are deemed Secure Electronic Messaging only when secure encryption is employed for those messages.

**University Electronic Messaging Systems** are electronic messaging systems or services provided by the University or any of its sub-units.

**Yale Personnel** are faculty, staff and students of Yale University and any others registered in the Yale Human Resources database whose appointment entitles them to a University email account.

Please also refer to the Master Glossary of HIPAA Security Terms in the Definitions section within Policy [5100](#) Electronic Protected Health Information Security Compliance.

---

## Policy Sections

---

### **5123.1 Reasonable and Appropriate Security Measures**

PHI may be electronically transmitted only when using reasonable and appropriate security measures in accordance with this policy. Generally, the greater the quantity, specificity or sensitivity of the PHI being transmitted, the more secure the means of transmission must be. Except for unusual emergency circumstances, with no feasible alternative mode of communication, information relating to HIV/AIDS, mental health or substance abuse that includes information that could be used to identify the individual may only be transmitted electronically using Secure Electronic Messaging (See Disclosure of De-identified Information and of Limited Data Sets referenced in Related Information below.)

Electronic Messages originating from Covered Components must include a privacy statement notifying the recipient of the insecurity of electronic messaging and of whom to contact should the message be misdirected. (see sample statements in [5123 PR 1](#)). Misdirected messages must be documented in the Accounting for Disclosures log upon notification of the message being misdirected (please see Accounting for Disclosures policy identified below under Related Information).

---

### **5123.2 Communications between Yale Electronic Messaging Systems and Yale New Haven Health System Electronic Messaging Systems**

PHI may be exchanged between Yale and Yale New Haven Health System personnel using electronic messaging provided that the electronic message remains wholly on institutionally managed Electronic Messaging Systems and the connection to those systems are secured (see connection standards in Data Network Access policy and procedures identified below under Related Information). By way of illustration, using a secure connection, e-mail between or among yale.edu and ynhh.org addresses is considered Secure Electronic Messaging.

### **5123.3 Electronic messaging between Yale personnel and external treatment providers**

Electronic communication of PHI between Yale personnel and external treatment providers is permitted using Secure Electronic Messaging.

Subject to 5123.1, PHI may be sent electronically without encryption between Yale personnel and external treating clinicians only if (1) the PHI does not include highly sensitive information, (2) all the following direct patient identifiers have been removed: name, date of birth, age if over 89, street address, phone number, fax number, e-mail address, and social security number, and (3) the PHI conforms to the minimum necessary standards (See Policy [5037](#) Minimum Necessary Uses, Disclosures and Requests under Related Information),

---

### **5123.4 Electronic messaging between Yale personnel and patients**

Electronic communication of PHI between Yale personnel and patients is permitted using approved Secure Electronic Messaging. A patient contacting his/her physician with a request for PHI could be referred to an approved Secure Electronic Messaging System to obtain an electronic response.

Insecure Electronic Messaging may be used with patients for communicating PHI that has minimal privacy-related consequences such as appointment reminders and notification of services such as flu shots. Also, until such time as an electronic medical record with integrated Secure Electronic Messaging or equivalent system is available, Yale Personnel may use Insecure Electronic Messaging to consult with patients including ePHI under the following conditions:

1. The patient must request such electronic communications in the context of other options and provide informed consent to the email exchange by an email acknowledgement such as provided in [5123 PR1](#) or equivalent.
2. While a patient may request electronic communication, the provider is not obligated to respond electronically and such response must be done with care: if the provider has any concerns about the legitimacy of the email query or the identity of the email correspondent, the provider must seek additional identifying information or refer the patient to a phone or in-person consultation.
3. The ePHI in any such communication must be the minimum necessary and in no event can include highly sensitive PHI such as information relating to HIV/AIDS, mental health or substance abuse.

---

### **5123.5 Electronic messaging between Yale personnel and non-Yale individuals, research subjects or organizations**

When the exchange of PHI is permissible under Yale's HIPAA policies, it may be exchanged between Yale personnel and non-Yale individuals, research subjects or organizations only using Secure Electronic Messaging.

---

### **5123.6 Use of the Yale University Voice Mail for communication of protected health information**

If any PHI might be left on an individual's University voice mail, that individual may not use the default password and must select a strong password.

---

## **Special Situations/Exceptions**

Units of the Covered Components (e.g. Yale University Health Services) 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 ePHI.

## Related Information

Policy [1610](#): Data Network Access Policy

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 [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.

---

## 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

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.

---