

**HIPAA Procedure 5123 PR.1**  
**Electronic Communication of ePHI**  
Revision Date: 04/20/05

---

<b>Electronic Mail Communication of PHI.....</b>	<b>1</b>
Overview .....	1
Definitions .....	1
General Guidelines .....	1
Approved Secure Electronic Messaging Options (end-to-end encryption): .....	2
Other electronic messaging options.....	2

---

## **Electronic Mail Communication of PHI**

### **Overview**

This procedure is designed to help insure the security and privacy of electronic Protected Health Information (ePHI) communications within the Yale University community and between members of the Yale University community, patients, research subjects and others outside the Yale community. This procedure assists in the implementation of Policy 5123: Electronic Communication of Health Related Information and should be read in conjunction with that policy.

---

### **Definitions**

**End-to-end Encryption:** When an electronic message is sent, it is securely encrypted in such a way that only the intended recipient can decrypt it. The message remains encrypted from when it enters the messaging system for transmission and is only decrypted when delivered to the intended recipient and upon presentation of that recipient's secret code.

**Instant Messaging:** A type of peer-to-peer (P2P) communications technology that enables an individual to create a private chat room with another individual. Typically, the instant messaging (IM) system alerts the individual whenever somebody on that individual's private list is online. The individual can then initiate a chat session with the other person. There are several problems with public IM networks, foremost of which is that the messages are not encrypted, allowing messages to be intercepted. Another security problem with public IM networks is that clients do not authenticate against a known source, such as Yale NetID and password or an Electronic Medical Record identify system.

**Secure Web site:** HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a secure connection from a Web browser to a Web server such as a web-based email service.

**SSL/TLS:** Secure Sockets Layer, also called Transport Layer Security (TLS), is a method of encrypting data when the data is transferred between computers over a network. The data is decrypted by the receiving computer during reception and is stored in an unencrypted form. This is referred to as "encryption over the wire" as opposed to "end to end encryption".

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

---

### **General Guidelines**

1. Any email containing PHI must contain the **Email Notice** (available at the HIPAA email guidance site at: <http://hipaa.yale.edu/guidance/emailconfidentiality.html> ).
2. Great care should be taken when sending an email with PHI to ensure that the recipient address corresponds to the intended recipient.
3. Any email containing PHI that is misdirected must be documented (See Policy [5003](#) – **Accounting for Disclosures**).

4. Email systems used by Yale University personnel must be configured to require **SSL/TLS** encryption when transmitting an email message to the SMTP server AND when retrieving messages from an IMAP or POP server (*contact your local IT support person for assistance*).
5. Except where PHI relates specifically to treatment, any PHI transmitted by email should be limited to the minimum necessary to meet the recipient's needs. (See Policy [5037](#): **Minimum Necessary** Uses, Disclosures and Requests).
6. Email messages containing PHI **must not be forwarded to non-Yale email addresses** either individually or by an automated forwarding mechanism unless an approved Secure Electronic Messaging option is employed (end-to-end encryption).
7. **Instant Messaging** (IM) software should not be installed or used for electronic messaging until an approved secure Instant Messaging (IM) option is available.

---

### **Approved Secure Electronic Messaging Options** (end-to-end encryption):

1) **POL**: Patient Online® is a secure, Web-based application allowing patients or research subjects to view portions of their medical record and electronically communicate with their clinicians. For further information visit [www.yalepatientonline.org](http://www.yalepatientonline.org)

2) **Yale File Transfer Facility** (<https://transfer.med.yale.edu/>): File transfer facility utilizes a secure web-based method for the actual data transfer, but retains the flexibility of email for the communications. This facility uses https--all transactions are encrypted. This encryption ensures that the data cannot be intercepted in transit. Retrieval of the file(s) to the intended individual should be restricted by providing a username/password pair that the recipient must know in order to retrieve the data:

*Do not send the password via File Transfer facility*

- Call the recipient to communicate the password
- Use a clue that only the recipient would know, such as “the password is your Mother’s maiden name” or “the password is the color of the scarf you wore last night”

---

### **Other electronic messaging options**

Yale policies permit provider to patient communication via email using Secure Electronic Messaging. In some circumstances, these policies also permit provider-to-patient email using insecure communications, but even in those circumstances only if requested by the patient and the patient provides informed consent with knowledge of alternatives (please see Policy [5123](#) Electronic Communication of Health Related Information).

A provider may obtain informed consent from a patient via email by presenting a consent message substantially similar to that described at the [HIPAA email guidance page](#).

Note that Policy [5123](#) places a set of constraints around such communications which include extra care by the provider to assure that the provider is confident of the correspondent’s identity and that any PHI be kept to a minimum. Further, even when requested by a patient, the provider should decline to use email and refer to phone or office visit if she or he has any concerns about any aspect of the exchange.

---

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.

---