



# University of Connecticut Health Center

**POLICY NUMBER 2004-01**

**May 20, 2004**

## **POLICY: ELECTRONIC COMMUNICATION OF PROTECTED HEALTH INFORMATION: USE OF UCHC SECURE MESSAGING PORTAL**

**PURPOSE:** To protect the confidentiality and privacy of protected health information (PHI) of patients/human subjects when the information must be communicated between providers and patients/human subjects via electronic means rather than in person or via mail delivery.

**SCOPE:** The information in this document applies to UConn Health Center (UCHC) employees granted access to Secure Messaging. Secure Messaging is a UCHC-developed system which provides electronic messaging functionality in a secure, encrypted mode for use in communicating PHI with patients and human subjects.

### **POLICY STATEMENT:**

UCHC is committed to safeguarding PHI in order to fulfill its mission to patients/human subjects, and to operate in a manner that is consistent with applicable federal and state laws and regulations. This policy defines guidelines and procedures that must be followed when communicating PHI electronically.

1. Because unencrypted electronic communications containing PHI could be a violation of the Health Insurance Portability and Accountability Act (HIPAA) laws, all UCHC employees granted access to Secure Messaging may only send communications to patients/human subjects using Secure Messaging. Internal uhc.edu and uchp.org e-mail may not be used to communicate PHI with patients/human subjects, unless they are UCHC employees with a uhc.edu or uchp.org e-mail address.
2. If a clinician receives an e-mail from a patient who is not an employee, the patient should be notified that the clinician can only respond via Secure Messaging. Procedures for participating in Secure Messaging should be provided to the patient.
3. Strict compliance with the Computer Use and Information Security policies is required when sending messages via Secure Messaging.
4. User names and passwords for access into the Secure Messaging portal are prohibited from being shared. A password is an electronic signature and is comparable to a written legal signature.
5. Secure Messaging is intended for use only in non-emergent medical situations.
6. All users of Secure Messaging are reminded that Secure Messaging must not be used for HIPAA defined "marketing" efforts aimed at patients/human subjects. Users of Secure Messaging are prohibited from attaching drug company, vendor, or business web addresses to patient communications. Educational Web sites and

- health care information Web sites may be referenced. See HIPAA Marketing Compliance UCHC Policy # 2003-05.
7. HIPAA restricts PHI that is shared between providers to be only the minimum necessary to accomplish the purpose of the disclosure. Only other providers who are or will be directly involved in the patient's care should be included in any communications.
  8. Electronic communication with patients is considered treatment and therefore is considered a part of the individual's medical record. As such, these communications will be released as allowed by applicable law with any valid requests for copies of the patient's record.

Iris Mauriello (signed)	6/23/04
<hr/>	<hr/>
<b>Privacy Officer</b>	<b>Date</b>
Sandra Armstrong (signed)	6/23/04
<hr/>	<hr/>
<b>Chief Information Officer</b>	<b>Date</b>
Peter J. Deckers (signed)	7/1/04
<hr/>	<hr/>
<b>Executive Vice President for Health Affairs</b>	<b>Date</b>

**Replaces: NEW POLICY**

References:

UCHC Computer Use Policy  
UCHC Information Security Policy  
UCHC Minimum Necessary Data Policy  
UCHC policy: E-mail: Use and Disclosure of Protected Health Information  
UCHC Policy: HIPAA Marketing Compliance  
AMA Guidelines for Physician-Patient Electronic Communications 5/16/03

Effective Date: May 20, 2004