



University of Connecticut Health Center

POLICY NUMBER 2003-22

April 16, 2008

POLICY: E-MAIL: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (Privacy & Security of Protected Health Information (PHI))

PURPOSE:

To protect the confidentiality and privacy of patient information when this information must be released via e-mail rather than by hand delivery or mail.

SCOPE:

The information in this document applies to all UCHC faculty, staff, students, volunteers and any other contractors or agents granted access to PHI.

Policy Statement:

UCHC is committed to safeguarding patient information in order to fulfill its mission to patients, and to operate in a manner that is consistent with applicable federal and State laws and regulations. This policy defines the guidelines and procedures that must be followed when transmitting or receiving e-mail regarding patients.

Guidelines/Procedures:

1. Patient information should be hand delivered or mailed whenever possible. However, emailing of patient information internally to authorized personnel within the UCHC system is allowable to facilitate treatment, payment and health care operations, provided the guidelines outlined in this policy are adhered to. Information transmitted must be limited to the minimum necessary to meet the requester's needs.
2. In recognition of the special communication needs of the deaf patient population at UCHC each deaf patient will be asked to provide an email address. This address will be entered into the IDX Registration application under "Email appointment communications." Communications using email will be limited exclusively to the deaf patient population and to information pertaining to appointment reminders and/or necessary changes to already established appointments for this select group of patients. No PHI will be shared in these email communications.
3. UCHC employees may e-mail PHI to other UCHC employees only. These e-mails can only be sent from and to secure e-mail addresses within the UCHC network. UCHC defines a secure e-mail address as one that ends with uhc.edu. E-mails of PHI cannot be sent unless the recipient

address can be verified as being secure.

4. All persons who send PHI via email should be aware of the following points:

- E-mail containing PHI must be treated with the same degree of privacy and confidentiality as the patient's medical/dental record.
- Confirm that the receiver has a need to know the information and is authorized to receive it.
- Send only the minimum necessary PHI to meet the intent of the request.
- Double check all recipient names/addresses to verify the correct person(s) will receive the email. (Be particularly sensitive to persons with the same last names/similar addresses.)
- In the event of a misdirected e-mail, the sender should direct the recipient to immediately delete the e-mail by: holding down the Shift key and clicking Delete on the closed message; this bypasses sending message to deleted items folder.

5. If an e-mail that contains PHI is received in error, the recipient should notify the sender and immediately delete the e-mail by hitting alt-delete.

6. All provisions of the UCHC Information Technology Computer Use and Security Policy must be observed with regard to access, use, modification, creation, disclosure, storage, copying, transmission, or destruction of information in any way related to online patient communications or interactions.

No Right to Privacy

UCHC encourages the business use of e-mail to increase productivity. The e-mail system and all the messages generated by e-mail, including backup copies, are part of the business infrastructure of UCHC, are owned by UCHC, and are not the property of the individuals who use the system as specified in UCHC's Computer Use Policy.

Right to Monitor, Audit, Read

As outlined in the UCHC Computer Use Policy, UCHC reserves the right to monitor, audit, and read e-mail messages.

References:

UCHC Computer Use Policy

UCHC Information Security Policy

UCHC Minimum Necessary Data Policy

eRisk Sample Policies and Disclaimers, A Work Product of the eRisk Working Group for Healthcare, c/o Medem, Inc. San Francisco, November 2000.

eE-Risk for Providers, Understanding and Mitigating Provider Risk Associated with Online Patient Interaction, Medem, Inc., San Francisco, March 2001

HIPAA Patient Privacy Compliance Guide, Safeguarding Protected Health Information, Chapter 2500, January 2002

| | |
|---|-------------|
| Iris Mauriello (signed) | 5/8/08 |
| <hr/> | <hr/> |
| Corporate Compliance Integrity/Privacy Officer | Date |
| Jonathan Carroll (signed) | 5/13/08 |
| <hr/> | <hr/> |
| Information Security Officer | Date |
| Peter Deckers, M.D. (signed) | 5/14/08 |
| <hr/> | <hr/> |
| Executive Vice President for Health Affairs | Date |

Originally Issued: April 14, 2003

Updated: April 16, 2008

Reviewed: April 16, 2008