THE UNIVERSITY OF CHICAGO
HIPAA Program Office

GUIDANCE October 31, 2008

EXECUTIVE SUMMARY
E-MAIL COMMUNICATIONS: INCLUDING PHI IN E-MAIL

The University of Chicago Medical Center (UCMC) supports the timely e-mail communication of protected health information (PHI) to promote patient health and safety and efficient customer service while balancing the need for patient privacy. As such, e-mail communication involving PHI is allowed only under specific circumstances, and shall occur according to UCMC guidelines.

It is recommended that you refer to the specific guidelines when sending PHI in E-Mail. The guidelines *(See link #1 on page 2)* are in *question and answer* format and also include scenario based information related to E-Mail communication:

1. Within UCMC/BSD
2. With External Entities (e.g. vendors, insurance companies)
3. Between UCMC Provider and Non-UCMC Providers

At this time, UCMC does not have an "organizational-wide" secure e-mail messaging system for e-mail communication sent outside UCMC. E-mail sent via the Internet or other unsecure means can be intercepted and read by individuals other than the intended recipient. This poses a risk to our patients and UCMC.

In order to minimize risks of violating our patients' privacy, individuals should follow these principles when sending PHI via e-mail:

1. Only use your UCHospitals, BSD, or departmental e-mail addresses. Do not send PHI to or from your Hotmail, Yahoo, or personal e-mail accounts.

2. Only send e-mail to individuals directly involved with the specific content of the e-mail (*send to individuals with a need to know*).

3. Do not use "patient specific information" such as the patient's name, initials or medical record number in the subject line of the e-mail.

4. Limit e-mail containing PHI to the minimum necessary information to meet the intended purpose.

5. Check that all address fields (e.g. "to", "cc", and "bcc") reflect the correct individuals who will receive the message.

6. Do not send attachments containing PHI via unsecure email (e.g. internet).

7. Contact the Chicago Biomedicine Information Services (CBIS) Department at 2-3456 for information on establishing a secure method for transmitting sensitive information via email. Such approved methods include Virtual Private Network (VPN), Secure File Transfer Protocol (sFTP), and the WebShare Service *(See link #2 on page 2)* available from the University of Chicago – Networking Services & Information Technologies (NSIT).

NOTE: A separate EXECUTIVE SUMMARY *(See link #3 on page 2)* exists for the guidance – **"E-Mail Communications Between UCMC Providers and Patients."** *(See link #4 on page 2)*

For more information, please contact the HIPAA Program Office at 4-9716

GUIDANCE October 31, 2008

EXECUTIVE SUMMARY

E-MAIL COMMUNICATIONS: INCLUDING PHI IN E-MAIL

Links Referenced in this Document

1. E-mail Communications Guidelines: Including PHI in E-mail
   http://hipaa.bsd.uchicago.edu/General_Email_Guidelines.pdf

2. NSIT's Webshare Services Summary Document
   http://hipaa.bsd.uchicago.edu/NSIT_WebShare_Services_Summary20080215_FINAL.pdf

3. Executive Summary: Between UCMC Providers and Patients E-mail Guidelines
   http://hipaa.bsd.uchicago.edu/Executive_Summary_Provider_Patient_Email_Guidelines.pdf

4. E-mail Communications Guidelines: Between UCMC Providers and Patients
   http://hipaa.bsd.uchicago.edu/Email_and_PHI_Guidelines_Provider_Patient_Grid.pdf