

EXECUTIVE SUMMARY

E-MAIL COMMUNICATIONS BETWEEN UCMC PROVIDERS & PATIENTS

Many University of Chicago Medical Center (UCMC) patients appreciate being able to communicate with their physicians via e-mail. The option to communicate via e-mail can influence a patient's perception of his or her overall patient care experience. 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.

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. While most patients who use e-mail are savvy about the risks, this does not absolve UCMC physicians and other personnel from using caution and good judgment about content that is appropriate for e-mail.

The HIPAA Steering Committee, in consultation with faculty members who have an interest in this topic, has established guidelines for communicating with patients via e-mail (*See link #1 on page 2*). The guidelines, which are in *question and answer* format, are intended to protect our physicians and patients by minimizing the risk of inadvertent disclosure of PHI.

1. E-mail is forever.
2. E-mail is a unique mode of communication that is best suited to brief discussions about straightforward topics. Always limit conversation to the "minimum necessary."
3. Medical advice that is communicated via e-mail should be documented in the medical record. See Q5 in the Guideline (*See link #1 on page 2*) document for more information on how to do this.
4. The patient should initiate e-mail relationships with the physician. The physician should set ground rules and expectations (e-mail is not for emergencies, etc.). See Q3 in the Guideline document for more information (*See link #1 on page 2*).
5. Only use your UCHospitals, BSD, or departmental e-mail addresses. Do not send PHI to or from your Hotmail, Yahoo, or other personal e-mail accounts.
6. Avoid e-mail correspondence that involves "highly confidential information" (HCI) (e.g. mental health, HIV/AIDS). Never initiate an e-mail discussion involving HCI. You may respond to a patient question initiated via email about HCI. Use professional judgment about whether another form of communication is more appropriate (e.g. phone call or medical appointment).
7. Put "**Confidential: Doctor-Patient Information – For Authorized Individuals Only**" in the subject line so it is clear that the information is confidential and should be viewed only by authorized individuals.
8. Avoid sending attachments (e.g. lab results, clinic notes) containing PHI via unsecure email (e.g. Internet). Contact the Chicago Biomedicine Information Services (CBIS) Department at 2-3456 for information on WebShare (*See link #2 on page 2*), a secure method for transmitting PHI via email.

NOTE: A separate EXECUTIVE SUMMARY (*See link #3 on page 2*) exists for the guidance – "**E-Mail Communications: Including PHI in E-mail.**" (*See link #4 on page 2*)

EXECUTIVE SUMMARY
E-MAIL COMMUNICATIONS BETWEEN UCMC PROVIDERS & PATIENTS

Links Referenced in this Document

1. E-mail Communications Guidelines: Between UCMC Providers and Patients
http://hipaa.bsd.uchicago.edu/Email_and_PHI_Guidelines_Provider_Patient_Grid.pdf
2. NSIT's Webshare Services Summary Document
http://hipaa.bsd.uchicago.edu/NSIT_WebShare_Services_Summary20080215_FINAL.pdf
3. Executive Summary: Including PHI in E-mail Guidelines
http://hipaa.bsd.uchicago.edu/Executive_Summary_to_General_Email_Guidelines.pdf
4. E-mail Communications Guidelines: Including PHI in E-mail
http://hipaa.bsd.uchicago.edu/General_Email_Guidelines.pdf