HIPAA Policy Summary – Sending PHI in Email

The University's Safeguards Policy covers three main areas of HIPAA compliance. The focus of this summary is Technical Safeguards, specifically email**.** The University is required to have in place reasonable safeguards to (1) limit access to e-PHI to authorized individuals and (2) protect against unauthorized disclosures of e-PHI. These safeguards include, at a minimum, those below. Each HCC, however, must put in place additional safeguards, based on the clinic or area technology used, operations, types of services provided, and nature or information maintained.

1. **Sending Email Containing PHI within the University or to OU Medical Center**
    a. Email from an OUHSC.EDU, OU.EDU, or HCAHealthcare.com email address to an OUHSC.EDU, OU.EDU, or HCAHealthcare.com email address is secure. However, content should be limited to the minimum necessary or a limited data set.
    b. Within the University, PHI may be emailed only to another University Health Care Component unless you have patient Authorization or the disclosure is for treatment, payment or operations.
    c. The recipient's name and email address should be verified before the message is sent.

2. **Sending Email Containing PHI Outside the University or OU Medical Center**
    a. Except in a documentable emergency, sending an email containing PHI to a non-OUHSC.EDU, non-OU.EDU, or non-HCA email address is prohibited unless:
        1. The message is encrypted between the sender and recipient in a manner that meets the legal requirements (consult your IT professional if you are not sure), or
        2. The message is sent using the University's Secure Messaging or Secure Email program.
    b. Content should be limited to the minimum necessary or a limited data set.
    c. The recipient's name and email address should be verified before the message is sent.

3. **Responding to Email from Outside the University or HCA that Requests PHI***
    a. If you receive an email from a patient or other individual from a non-OU or non-HCA email address, you must:
        i. Decline to respond, if the individual has not set up a secure email/secure messaging account with the University or encryption is not used by sender and recipient (see sample response in Safeguards policy), or
        ii. Respond via a secure method, observing the minimum necessary standard or by limited data set, if the email is received through one of the secure accounts or is otherwise encrypted.

*You are not required to send PHI by email, even if a patient or other individual requests the information be sent via email. You should never send PHI in a manner that you are not comfortable is secure.

All email containing PHI sent by University Health Care Components must include a Confidentiality Notice. A sample notice is included in the Safeguards policy, available on the University's HIPAA webpage.