Protecting HIPAA PHI in E-Mail - Did you know…?

Did you know that all emails containing PHI sent outside the organization must be encrypted, unless the patient (or research subject) specifically request it to not be. In this case, you must advise the patient that there are risks to their information being inappropriately accessed or disclosed when sent unencrypted. If the patient agrees to assume that risk, you must document this in their Epic record and may then proceed to send the email unencrypted as requested. *Only the patient can agree to this risk* Third parties cannot accept this risk on behalf of the patient.

Email Encryption

Emails sent to the following domains are automatically encrypted:

- @cuanschutz.edu (CU Anschutz)
- @ucdenver.edu (CU Denver)
- @cumedicine.us (CU Medicine)
- @cuhealth.org (CU Health)
- @denverhealth.org (Denver Health)
- @nationaljewish.org (National Jewish Health)
- @childrenscolorado.org (The Children's Hospital of Colorado)
- @uchealth.org (UCHealth)

To ENCRYPT, Add the Word "SECURE" to the Subject Line…

- When emailing **Excel spreadsheets containing lists** of patient/research subject names, addresses and test results
- When attaching **Word or PDF documents with letters to patients** advising of research study inclusion/exclusion status
- When **emailing with a consulting provider out-of-state** referencing a specific patient/research study participant
- When an email buried deep in the **thread contains patient-specific information (PHI)** – add SECURE to the Subject Line
- **When in doubt**, add "SECURE" to the Subject Line!

For emails ending in any other domain (i.e., @ABChospital.org), you must take extra steps to encrypt messages containing PHI.

To send encrypted email, add one of the following words in all capital letters to the SUBJECT line.

- ENCRYPT (CHCO)
- SECURE (University, UCHealth)