Subject: E-MAIL --- THE LAW & YOUR RESPONSIBILITY

Sending e-mail messages with sensitive information (patient, confidential or other personal identifying information) without the appropriate safeguards can violate HIPAA and/or North Carolina Identity Theft regulations.

Compromised sensitive information can lead to costly civil penalties, criminal penalties, negative personal impact to individuals affected, costs to notify individuals affected, and very likely a long-lasting impact to UNC Health Care and School of Medicine’s reputations.

Sending/Forwarding sensitive information to outside e-mail addresses

If you deal with sensitive information via e-mail, you should not forward those messages (automatically or manually), to accounts such as Gmail or YahooMail which are outside of the UNC Health Care system and the School of Medicine system.

If you need to send e-mail messages containing sensitive information to non-UNC Health Care or School of Medicine e-mail addresses, see the appropriate link below for specific requirements and instructions for securing e-mail:

- **UNC School of Medicine E-mail Users**
  

- **UNC Health Care and UNC Hospitals E-mail Users**
  
  [http://intranet.unchcare.org/hospitaldepartments/isd/sending-secure-e-mail](http://intranet.unchcare.org/hospitaldepartments/isd/sending-secure-e-mail)

Unintended recipients

Before sending a message that contains sensitive information, check to make sure there are no unintended recipients, especially when forwarding a message or when using "Reply All." When using an "auto fill" feature where a full e-mail address is inserted based on the first few letters that you type, make sure the e-mail address that is filled in is actually the one you intended to use.

Excessive personal use

While incidental and occasional personal use of a UNC Health Care / School of Medicine e-mail account is permitted, try to keep work e-mail and personal e-mail in separate accounts. Personal use of your work e-mail address increases the chances that malicious software could infect your work computer or that sensitive information could be accidentally passed on to an unauthorized individual.