UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Emailing and Transmitting PHI	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Revised:** 11/15//2016; 3/22/2017; 4/1/2018, 2/15/19, 7/22/22, 2/16/24, 4/1/25, 10/23/25

I. PURPOSE

To ensure Protected Health Information being transmitted electronically is protected from unauthorized Access.

II. POLICY*

This policy applies to all Health Care Components of both campus Covered Entities that transmit PHI from any electronic media device, including but not limited to desktop computers, laptop computers, tablet computers, digital copiers, scanners, and smart phones. Each HCC shall require that its Workforce Members comply with the following:

A. Electronic Transmissions - Each Health Care Component shall have in place written procedures for emailing PHI consistent with the following:

1. Minimum Necessary - Workforce Members shall observe the Minimum Necessary Rule when transmitting PHI, meaning they will send only the PHI necessary at that time.

2. Subject Line - Workforce Members shall not include PHI in the subject line of any electronic transmission. (Subject lines are not generally encrypted and are visible even on unopened messages.)

3. Email Within the University Email Systems - Sending emails that contain PHI for an authorized purposes within the University email systems (OUHSC.edu/OU.edu to OUHSC.edu/ou.edu) to an individual authorized to receive the PHI is acceptable. PHI should be sent as a limited data set when possible. The Minimum Necessary Rule must be observed when applicable (see HIPAA *Minimum Necessary Rule* policy). Workforce Members do not need to use [secure] or [OUENCRYPT] when transmitting emails within the University Email Systems but should validate the proper recipient and that there no recipients outside the University email systems are included prior to sending. If the email transmission includes recipients outside of the University email system, follow the procedures below (Section II.A.5).

4. Email Between OU.edu/OUHSC.edu and oumedicine.com or ouhealth.com E-mail Addresses - Sending emails that contain PHI for an authorized purpose between OU.edu/OUHSC.edu and oumedicine.com or ouhealth.com email addresses is secure and therefore acceptable so long as the recipient is authorized to receive the PHI. PHI should be sent as a limited data set when possible and in accordance with the Minimum Necessary Rule, as applicable. Workforce Members do not need to use [secure] or [OUENCRYPT] when transmitting emails to oumedicine.com but should validate the proper recipient and that no recipients outside the University email systems or oumedicine.com system are included prior to sending. If the email transmission includes recipients outside of the OU.edu/OUHSC.edu, oumedicine.com, or ouhealth.com email domain, follow the procedures below (Section II.A.5).

5. E-mail Outside the University Email Systems - Email may be used to send PHI to an authorized recipient outside the University email systems (OU.edu/OUHSC.edu) only for an authorized purpose to an authorized recipient. In all cases, the message must be encrypted between sender and recipient in a manner that complies with HIPAA. Contact OU IT to confirm an encrypted (TLS) channel has been established with the recipient's email domain. If an encrypted channel does not exist, other options for secure transmissions include, for example, typing in the subject line **[secure]** for Health Campus email accounts or **[OUENCRYPT]** for Norman Campus email accounts.

6. Email to Patients - Workforce Members must comply with this policy, as well as with the policy or practice of their HCC. (A HIPAA *Consent for Electronic Communication* form is available on the HIPAA website. Sample language for responding to requests from patients requesting that their PHI be sent via an unencrypted method is available below.) For OU Physicians, for example the preferred method for communicating electronically with patients is through a secure patient portal.

    a. When E-mail Encryption is Available. Subject to the Health Care Component's internal policies and procedures, Workforce Member may send PHI to patients via encrypted email for permitted purposes to authorized recipients.

    b. Without Encryption Capabilities (E-Mail Communication Denial). If a patient sends an e-mail to an employee, student/trainee, or volunteer asking a health care question or requesting any type of information that would require a Disclosure of PHI without encryption, the request for response shall be declined by sending a new message (not a reply) similar to the following:

    "I have received your health care question or request for health information. However, I cannot respond using e-mail because to do so would require the transmission of information that I consider to be personal or highly sensitive, and e-mails can be intercepted. I will respond to your question or request through some other means of communication. If you wish to receive health information via

email, please submit Consent for Electronic Communication form to your health care provider or log in to your patient portal account, if available."

Note: The HIPAA *Consent for Electronic Communication* form is available on the HIPAA forms webpage.

If a patient does not want to complete this form but insists on receiving PHI via unsecure (unencrypted) email, Workforce Member shall refer to their Health Care Component email procedure or refer the patient to the supervisor. The supervisor shall, or shall require personnel to, obtain written confirmation from the patient that the patient understands that the email will not be secure and may be intercepted by an unauthorized individual, but still wishes to receive the PHI via mail. The patient's written confirmation must be maintained in the patient's file for six (6) years.

7. E-mail Notice - All emails initiated by a Workforce Member that contain PHI must include a confidentiality statement similar to the following, typically below the signature line:

    i. *This email, including any attachments, contains information that may be confidential or privileged and is intended for use by the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the email and attachments.*

8. Text Messaging - Workforce Members may not send PHI via unencrypted text messaging unless the patient has consented in writing to receive an unencrypted text and the Workforce Member is permitted by the manager to do so. Otherwise, those who choose to use text messaging (SMS protocol) must de-identify PHI in the message or encrypt incoming and outgoing messages and ensure they use a secure gateway (e.g., HTTPS) if they send the messages over an Internet gateway. Workforce Members are cautioned that if the recipient does not have the **same** encryption protocol, the text may not be secure. IT Security can provide additional information.
   Do not take pictures or Screenshots of conversations in the secure texting portal.

   Note: Texting physician orders --encrypted or unencrypted-- is prohibited by CMS and the Joint Commission.

9. Text Pagers - Workforce Members shall exercise extreme caution when sending PHI via text pagers, as few pagers have encryption enabled. Consult IT Security.

10. Auto-Forwarding Email - Employees of Health Care components may not auto-forward email to a non-OUHSC.edu or non-OU.edu email address.

11. Digital Copiers/Scanners/Equipment - Health Care Components using digital copiers, scanners, fax machines, and medical and other equipment that transmits or stores PHI, even temporarily, must verify that appropriate data security features (e.g., encryption, overwriting) are enabled. In addition, before the equipment is returned to the vendor, transferred, surplussed, or otherwise disposed of, the Health Care Component must take steps to ensure the hard drive is destroyed or completely overwritten. These steps may include, but are not limited to, notifying the Purchasing Department to impose these requirements on the vendor during the contracting process or working with IT Security prior to retiring, disposing of, transferring, or surplussing the device to ensure the PHI is rendered unusable, unreadable, or indecipherable. (See HIPAA *Purchasing or Leasing Equipment or Contracting for Services Involving PHI* policy.)

B. Telemedicine

1. Workforce Members may use telemedicine technology if it meets AES Encryption standards for H.323 protocol communications, an IT Security Risk assessment has been completed and all associated risk have been addressed or mitigated and a contract through the University to include a Business Associate Agreement has been established.

2. Workforce Members shall be responsible for providing telemedicine patients with any required forms and the Notice of Privacy Practices, in a secure manner, prior to using this technology. Contact the Office of Legal Counsel for assistance.

Any questions about the security of electronic transmissions generally should be directed to IT Security or IT Representative supporting the HCC.

C. Electronic Documents - Documents and attachments and/or images containing PHI are required to be stored on University network servers with appropriate security restrictions in accordance with IT Security policy, rather than on portable devices or unsecure desktop computers. (IT Security can provide specific information about these servers.) If documents and attachments and/or images cannot be stored on a University network server or are but instead are stored on a desktop computer or portable computer device, **the Workforce Member must ensure** that the computer or device is encrypted, prior to storage, by contacting the appropriate IT Representative supporting the computer or device.

D. Other Uses/Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented to protect the PHI. Health Care Components and Workforce Members should contact IT Security or the HIPAA Security Officer for more information.

E. Social Media Sites. Protected Health Information shall not be posted or transmitted on social media sites, such as Facebook or Twitter. Replies to patient posts should be avoided, especially if the reply will confirm PHI. Workforce Member should keep in mind that even if a patient's name is not posted, if the patient could reasonably be identified, alone or with information obtained from other sources, the information is considered Protected Health Information. Do not use your personal social media account to discuss or communicate patient information with one of your patients, even if the patient initiated the contact or communication. Always use approved communication methods when communicating with patients about their health or treatment.

The HIPAA *Breach of Unsecured PHI/ePHI* policy and the HIPAA *Sanctions* policy shall be followed in the event a Workforce Member violates this policy, inadvertently or intentionally.

III. REFERENCES

A. 45 CFR 164.312(e)
B. HIPAA Administrative and Physical Safeguards; Minimum Necessary Rule, and Sanctions policies
C. Information Technology Secure Email and Cybersecurity Information - https://www.ou.edu/ouit/cybersecurity/policies/hsc-policies