MUSC Health
Medical University of South Carolina

HIPAA TIP SHEET

Employees of the Medical University of South Carolina are expected to protect patient information in accordance with HIPAA privacy and security rules. This is a fundamentally important aspect of all patient care for everyone. This tip sheet highlights key HIPAA focus areas. Many of the tips below are covered under policy C-003, *Patient Confidentiality Handbook*; please refer to that policy for additional information.

Access

The HIPAA rule allows access to the medical record for payment, treatment and healthcare operations. Any access outside of what is permitted is considered unauthorized, i.e. “snooping” and constitutes a HIPAA breach.
Examples of unauthorized access include viewing:

- anyone’s medical record out of curiosity or concern (e.g., Covid-19 results)
- a record of a celebrity or newsworthy patient
- a record of a patient you treated in the past, when you are not involved in their current treatment
- a record to look up an address, birthday or any other demographic information

Email

- Only send the “minimum necessary” protected health information (PHI)
- Always verify the recipient prior to sending
- Communication of sensitive tests and emergency information via email is prohibited

External:

- Use MyChart to communicate directly with patients **(Best Practice)**
- If a patient requests communication via private email:
  - Document the request in the medical record
  - Send a test message and have the patient reply
- Emails sent outside of MUSC must be encrypted.
  - Type **SEND SECURE** in the subject line of the email

Receiving Email:

- External email has a banner that says “Caution: External”
- **Never** respond to an email asking you for your user name and password; OCIO will never ask you for your user name and password via email
- If you need to respond to an external email chain with PHI in the message, you must encrypt that message (see above)

Mobile Devices

- In cases where texting and/or paging clinical information is the most appropriate means of communicating time sensitive information, the minimum amount of PHI necessary should be included in the text/page. Per CMS, all providers must use texting/communication platforms that are secure and encrypted. MUSC’s approved communication platform is the Simon paging system, which includes Spok mobile for your mobile device and MUSC’s encrypted pagers. When using approved technologies, contents related to patient care/treatment must be documented in the medical record.
- Beware of automatic cloud backup for sensitive information.
- If you plan to use a device for photos/videos, you must enroll in the Canto/Haiku app. Access to a patient’s medical record through Canto/Haiku is subject to the same restrictions as access to Epic or any other protected health information.
- Employees may use mobile devices for work purposes but must ensure that they follow the Mobile Devices Management policy and are required to use Two Factor Authentication.