## Patient Confidentiality/HIPAA Education

**We owe it to our patients:** Keeping patient information confidential is the responsibility of every employee, volunteer, physician and each member of our Health Care Team. A breach, compliance or confidentiality issue can be reported to the hotline at 380-0210 anonymously or to the HIPAA Privacy Officer, Candace Matheny at 251-460-5250.

- Ask the patient if it's permissible to discuss his/her care with a family member or other requestor before sharing any medical information. Document the patient's wishes. If speaking with someone over the phone, verify caller's identity & appropriateness by asking for the patient's unique 4 digit privacy code.
- Patient's Chart / Medical Record is a Legal Document of Information, whether paper or electronic. The information is protected by Alabama State and Federal Laws (HIPAA). The document is the business record of the facility/hospital.

- A patient's healthcare information should be accessible only to those who have a "need to know" to deliver care to that patient. Any other request should have a Release of Information form approved/executed by the patient prior to release.

  - ***"Bee Alert"*** -- Use this "buzz phrase" to remind coworkers to keep patient information confidential and not discuss patient information in inappropriate places (cafeteria, elevators, hallways, stairways, etc.).
  - For security purposes, our computer system tracks each time you access patient information. DO NOT access information unless you have a business need or are participating in the care of the patient.
- Patients who decide to opt out of the directory are considered "Confidential." In Sunrise a confidential flag is displayed. Do not inform anyone of the patient's presence in the hospital if this flag is present.
- Protected health information should never be disclosed to anyone unless they have a legitimate right to it. Confidential information should not be left in public places, thrown in the regular garbage, etc.
- Unauthorized access or disclosure of protected health information can result in monetary fines, for employees. If you disclose patient information by accident you are still responsible and must report the accidental disclosure to the Privacy Officer.
- Core privacy principles such as not discussing information about patients outside of SMC remain unchanged regardless of technologies or trends. Employees should never post patient related information on social media outlets such as Facebook or Twitter, as the potential for violating privacy laws increase when healthcare professionals engage in the use of social media.
- Should you be issued a company email account, Phishing emails are designed to trick victims into clicking on a link or opening an attachment that launches malware. To safeguard against phishing scams and malware you should delete suspicious email. Suspicious emails may include typos in the links contained in the email, claims of winning a contest, or requests to confirm personal information a sender should already have. Be sure not to conduct personal business on a Springhill computer or by providing your Springhill email address. When in doubt, forward the email to information.security@springhill.org, or if applicable, select the "Phish Alert" button in your email
- If your job requires you to correspond with contacts outside of the organization, and the communication involves the use of protected health information or sensitive company information, Springhill's Data Loss Prevention policy requires encryption of emails and data prior to sending. To encrypt an email, type **encrypt** in the subject line of the email or in the body of the email, or select "send securely" when sending.

Protected Health Information (PHI) includes information that can be used to identify the individual and relates to the health of the individual: ☑ Patient Name ☑ Social Security Numbers ☑ Date of Birth ☑ Telephone & Fax Numbers ☑ Medical Records & Account Numbers ☑ Relatives' Names ☑ Treatment Information ☑ Addresses ☑ Codes ☑ Photos ☑ Employers ☑ Occupation ☑ Email Addresses ☑ Payment Information ☑ Health Plan Beneficiary Numbers ☑ Certificate/License Numbers

- Core privacy principles such as not discussing information about patients outside of SMC remain unchanged regardless of technologies or trends. Employees should never post patient related information on social media outlets such as Facebook or Twitter, as the potential for violating privacy laws increase when healthcare professionals engage in the use of social media

Student Signature: _____Date:_____