Springhill Medical Center
Confidentiality and Security Agreement

As an employee, student, or volunteer, I understand and agree that I must hold medical and other patient information in confidence. I understand "Confidential Information" (i.e, medical records, surgery schedules, physician-patient correspondence, etc.) to mean any patient information which I have seen, heard, or acquired while within a facility owned or operated by Springhill Hospitals, Inc. d/b/a Springhill Memorial Hospital ("SMH") or obtained remotely from SMH's computerized patient information system(s). I further understand that I must sign and comply with this agreement in order to obtain authorization for access to Confidential Information.

1. I agree to access and use Confidential Information only when it is necessary to perform my job related duties and in accordance with SMH's Privacy and Security Policies.
2. I agree not to discuss, reveal, copy or in any other manner disclose the contents of any Confidential Information, unless I am authorized to do so through an appropriate and properly executed "request for release of medical information" and it has been determined and ordered by the appropriate authority that the information is to be released, or the necessary authorization and consent has been obtained from the patient.
3. I understand that medical records, whether in paper or electronic form, are confidential and I agree to comply with all state and federal laws and regulations related to patient information including the Standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996, as any of such laws and regulations may be amended from time to time.
4. I understand that any information concerning a patient obtained during the course of my affiliation with SMH is Confidential Information, and that I have the responsibility for safeguarding the Confidential Information regardless of whether the patient is currently receiving medical services from SMH.
5. I agree to maintain the confidentiality of the Confidential Information both in and outside of SMH.
6. I understand that disclosure of Confidential Information to persons other than authorized health care professionals may be an invasion of a patient's privacy rights and is of a personal and private nature.
7. I agree to take all reasonable precautions to prevent the unauthorized disclosure of any Confidential Information and will destroy such appropriately.
8. I will:
    a. Use only my officially assigned SMH User-ID and password.
    b. Maintain the confidentiality of my SMH password.
    c. Notify the SMH IT&S Department of a breach in security of my SMH password.
    d. Notify the SMC IT&S Department of any suspected or confirmed breach of PHI.
    e. Not attempt to learn the password of any other authorized user of the Information System.
9. I will never:
    a. Share/disclose my SMH User-ID and/or password with anyone, not even family members or coworkers.
    b. Use tools or techniques to break/exploit SMH's security measures.
    c. Connect to unauthorized networks through the Information System or an SMH device.
10. I will immediately report to SMH, in writing, any use and/or disclosure of Confidential Information that is not permitted by this agreement of which I become aware.
11. I will practice good workstation security measures, i.e. not leaving the Information System up with patient information when away from desk, pointing screens away from public view.
12. I will only access or use the Information System or an SMH device that I am officially authorized to access or use, and will not demonstrate the operation or function of the Information System or an SMH device to unauthorized individuals.
13. I understand that violation of this agreement may result in disciplinary action by my employer, up to and including termination of employment.
14. I agree that my obligations under this agreement will continue after termination of my employment or my relationship ceases with SMH.
15. I agree to only request and access confidential information that is needed for purposes of patient care.
16. I understand and agree that SMH may, at any time and for any reason or no reason, restrict and /or permanently cancel my access into the Information System.
17. I hereby acknowledge that any and all information stored in, derived from, and/or accessed from the Information System provided by SMH is the sole property of SMH.

By signing this document, I acknowledge that I have read this agreement and I agree to comply with all the terms and conditions stated above.

Employee Signature	Date

HIPAA 1-2-3 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, Mary Jo Montgomery or HIM Director, Sharon Barnicle at 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.
- Protected Health Information (PHI) includes information that can be used to identify the individual and relates to the health of the individual: 1) Patient Name 2)Social Security Numbers 3) Date of Birth 4)Telephone & Fax Numbers 5) Medical Records & Account Numbers 6) Relatives' Names 7) Treatment Information 8) Addresses 9) Codes 10) Photos 11) Employers 12) Occupation 13) Email Addresses 14) Payment Information 15) Health Plan Identification Numbers 16) License Numbers
- For the patient's security, as well as yours, you should NEVER share your password with others. Access to confidential information is audited and your password/login determines the appropriateness of the access. Also, NEVER let anyone use your password to access or document information.
- Always sign off of the systems you are in before you leave your work area.
- 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: _____