Tidelands Health

Confidentiality Agreement

Employee Name (Please Print) _____

In consideration of my access to records maintained at Tidelands Health (GHS), whether in paper or electronic form, I agree to be bound by the following terms and conditions during my employment at Tidelands Health.

1. I understand that my computer password is unique to me. I will not disclose it, or permit others to use it. If my password becomes known to any other person or group by reason of disclosure, I shall inform Information Systems immediately. Use of the software or documentation provided by Tidelands Health is limited to the person authorized by this agreement. I will not remove any materials from the premises for use on any other computer.

2. GHS communication systems are considered Tidelands Health property and meant for business use only. Employees shall have no expectation of privacy while using company property, even if using a password. I understand that all communication systems and files are subject to monitoring. I understand that GHS is authorized to monitor oral, electronic and written communications for "business use only" purposes. GHS is permitted to monitor systems such as phone use, voice mail, computer network, and Internet use, and will also include other communication systems, as necessary. Non-business use of Internet or e-mail is prohibited.

3. Tidelands Health prohibits transmission, downloading, or access to offensive or improper (as determined by the Administrative Compliance Committee) material.

4. My authorization to use the electronic information systems at Tidelands Health is limited to specific information required in the performance of my duties. I understand that accessing phi in electronic or printed form for reasons other than treatment, payment, or operations is prohibited by federal HIPAA regulations.

5. I understand that any information I may access is to be kept strictly confidential and is the proprietary property of Tidelands Health.

6. Failure to comply with the terms hereof may result in disciplinary action up to and including termination of my employment with Tidelands Health.

7. I agree to abide by the confidentiality laws of the State of South Carolina and of the United States.

8. NEITHER THIS AGREEMENT NOR ANY PROVISION OF THIS AGREEMENT CONSTITUTES AN EMPLOYMENT CONTRACT OR ANY OTHER TYPE OF CONTRACT. YOUR EMPLOYMENT RELATIONSHIP WITH TIDELANDS HEALTH IS FOR AN INDEFINITE PERIOD AND EITHER YOU OR TIDELANDS HEALTH MAY TERMINATE THE RELATIONSHIP AT ANYTIME, FOR ANY REASON NOT PROHIBITED BY LAW.

Student Signature _____ Date _____

Print Name: _____

EXHIBIT A (GSRMC)

STATEMENT OF RESPONSIBILITY

For and in consideration of the benefit provided the undersigned in the form of experience in a clinical setting at Grand Strand Regional Medical Center, LLC d/b/a Grand Strand Regional Medical Center ("Hospital"), the undersigned and his/her heirs, successors and/or assigns do hereby covenant and agree to assume all risks and be solely responsible for any injury or loss sustained by the undersigned while participating in the Program operated by Horry Georgetown Technical College ("School") at Hospital unless such injury or loss arises solely out of Hospital's gross negligence or willful misconduct.

Signature of Program Participant/Print Name Date

Parent or Legal Guardian if Program Participant is under 18/Print Name Date

EXHIBIT B (GSRMC)

PROTECTED HEALTH INFORMATION, CONFIDENTIALITY, AND SECURITY AGREEMENT

- Protected Health Information (PHI) includes patient information based on examination, test results, diagnoses, response to treatment, observation, or conversation with the patient. This information is protected and the patient has a right to the confidentiality of his or her patient care information whether this information is in written, electronic, or verbal format. PHI is individually-identifiable information that includes, but is not limited to, patient's name, account number, birth-date, admission and discharge dates, photographs, and health plan beneficiary number.
- Medical records, case histories, medical reports, images, raw test results, and medical dictations from health care facilities are used for student learning activities. Although patient information is removed, all healthcare information must be protected and treated as confidential.
- Students enrolled in school programs or courses and responsible faculty are given access to patient information. Students are exposed to PHI during their clinical rotations in healthcare facilities.
- Students and responsible faculty may be issued computer identification (IDs) and passwords to access PHI.

Initial each to accept the Policy

Initial	Policy
	1. It is the policy of the school/institution to keep PHI confidential and secure.
	2. Any or all PHI, regardless of medium (paper, verbal, electronic, image or any other), is not to be disclosed or discussed with anyone outside those supervising, sponsoring or directly related to the learning activity.
	3. Whether at the school or at a clinical site, students are not to discuss PHI, in general or in detail, in public areas under any circumstances, including hallways, cafeterias, elevators, or any other area where unauthorized people or those who do not have a need-to-know may overhear.
	4. Unauthorized removal of any part of original medical records is prohibited. Students and faculty may not release or display copies of PHI. Case presentation material will be used in accordance with healthcare facility policies.
	5. Students and faculty shall not access data on patients for whom they have no responsibilities or a "need-to-know" the content of PHI concerning those patients.
	6. A computer ID and password are assigned to individual students and faculty. Students and faculty are responsible and accountable for all work done under the associated access.
	7. Computer IDs or passwords may not be disclosed to anyone. Students and faculty are prohibited from attempting to learn or use another person's computer ID or password.
	8. Students and faculty agree to follow Hospital's privacy policies.
	9. Breach of patient confidentiality by disregarding the policies governing PHI is grounds for dismissal from Hospital.

- I agree to abide by the above policies and other policies at the clinical site. I further agree to keep PHI confidential.
- I understand that failure to comply with these policies will result in disciplinary actions.
- I understand that Federal and State laws govern the confidentiality and security of PHI and that unauthorized disclosure of PHI is a violation of law and may result in civil and criminal penalties.

Signature of Program Participant/Print Name Date

Parent or Legal Guardian if Program Participant is under 18/Print Name Date

Conway Medical Center
CONFIDENTIALITY AND SECURITY AGREEMENT

I understand that Conway Medical Center and its affiliate organizations, (hereinafter "CMC") in which or for whom I work, volunteer or provide services, or with whom the entity (*e.g*., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information, CMC, has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of its patients' health information. Additionally, CMC must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information "Confidential Information").

In the course of my employment/assignment or association with CMC, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with CMC's Privacy and Security Policies, which are available from CMC. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.

2. I will not in any way divulge copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.

3. I will not discuss Confidential Information where others can overhear the conversation.

4. I will not make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information.

5. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with CMC.

6. Upon termination of any relationship with CMC, I will immediately return any documents or media containing Confidential Information to CMC.

7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with CMC.

8. I will act in the best interest of the CMC and in accordance with its Code of Conduct at all times during my relationship with CMC.

9. I understand that violation of this Agreement may result in the disciplinary action, corrective action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within CMC, in accordance with CMC's policies.

10. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

11. I understand that I should have no expectation of privacy when using the CMC information systems. CMC may access, review, and otherwise utilize information stored on or passing through its systems, including e-mail, in order to manage systems and enforce security.

12. I will practice good workstation security measures such as locking up diskettes when not in use, using hospital approved screen savers with activated passwords appropriately, and position screens away from the public view.

13. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved standards.

14. I will:
    a. Use only my officially assigned User-ID and password.
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
    d. Contact the Information Technology department if my password is accidentally revealed to request a new password.

15. I will never:
    a. Share/disclose user- IDs or passwords.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect to unauthorized networks through the systems or devices.
    d. Install unauthorized software on hospital computer systems.

16. I will notify my manager or appropriate Information Technology person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy, and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements are additional requirements for physicians using CMC systems containing patient identifiable health information (e.g., Meditech):

17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to CMC at the time of each access that I have the requisite patient consent to do so, and CMC may rely on that representation in granting such access to me.

18. I will only access patient information to the extent it is reasonable and necessary for me to treat a patient. The information that I review will be kept confidential, and I will only review so much of a patient's medical record as is necessary for me to render appropriate treatment. If I am given access to a patient's medical record due to a consult, emergency situation, or an on-call situation at which time I am not the patient's primary attending physician, I will only access that patient's information to the extent it is needed for me to render appropriate medical treatment. Under no circumstances will I access a patient's information without a patient's verbal or written consent or for whom I am not rendering medical treatment.

19. I will ensure that only appropriate personnel in my office will access the CMC's software systems and Confidential Information and that I will annually train such personnel on issues related to patient confidentiality and access.

20. I will accept full responsibility for the actions of my employees who may access the CMC's software systems and Confidential Information

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/Consultant/Vendor/Office Staff/Physician Signature	Facility Name	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name	