



Student Form

Email address: \_\_\_\_\_

First Name \_\_\_\_\_ Middle Initial \_\_\_\_\_ Last Name \_\_\_\_\_

SSN: \_\_\_\_\_ Birth date \_\_\_\_\_

Home Address \_\_\_\_\_ Phone # \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

Ethnicity (circle one): White-Non Hispanic      Black/African American      Hispanic/Latino

Hawaiian/Pacific Islander      American Indian/Alaska Native      Asian

(Check one) Male \_\_\_\_\_ Female \_\_\_\_\_

=====

Name of School \_\_\_\_\_

Name of Program (i.e. Nursing, Lab Tech) \_\_\_\_\_

Person at BH reporting to: \_\_\_\_\_ Facility \_\_\_\_\_

Training Start Date \_\_\_\_\_ Training End Date \_\_\_\_\_

Have you ever been Employed, served an Internship, Residency, or Clinical Rotation with any facility of Baptist Health Care?

Facilities include:

- Andrews Institute
- Atmore Community Hospital
- Baptist Health Care
- Baptist Home Health Care
- Baptist Hospital
- Lakeview Center
- Baptist Leadership Group
- Baptist Manor Nursing Home
- Baptist Medical Park-Nine Mile
- Baptist Medical Park-Navarre
- Cardiology Consultants
- Gulf Breeze Hospital
- Jay Hospital
- PCC Student Center
- Baptist Medical Group

If so, please list reason for leaving: \_\_\_\_\_

=====

Disclaimer: This form is the property of Baptist Health Care Human Resources. All information provided will be kept confidential and will only be used for the purposes of setting up identification in the Lawson and LMS system.

=====

**(for office use only)**

BHC Student Badge number: \_\_\_\_\_ LMS Password: \_\_\_\_\_

Exhibits A & B signed: Yes \_\_\_\_ No \_\_\_\_

Reviewed date: Background Investigation \_\_\_\_\_ Drug Screen \_\_\_\_\_ TB Test \_\_\_\_\_

**EXHIBIT A**

STATEMENT OF RESPONSIBILITY

For and in consideration of the benefit provided in the form of experience in evaluation and treatment of patients of Baptist Health Care Corporation ("Baptist"), the undersigned, his/her heirs, successors, and/or assigns, does hereby covenant and agree to be solely responsible for any injury or loss sustained by the undersigned while participating in the \_\_\_\_\_ Program operated by \_\_\_\_\_ ("School") at Baptist unless such injury or loss arises solely out of Baptist's gross negligence or willful misconduct.

Dated this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_

\_\_\_\_\_  
Program Participant

\_\_\_\_\_  
Witness:

\_\_\_\_\_  
Printed Name:

\_\_\_\_\_  
Printed Name:

**EXHIBIT B**

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, birthdate, admission and discharge dates, photographs, and health plan beneficiary number.
- Medical records, case histories, medical reports, images, raw test results, and medical dictations from healthcare facilities may be used for Student learning activities.
- Program Participants may be given access or exposed to PHI during their clinical rotations in Baptist facilities.
- Program Participants may be issued computer identifications (IDs) and passwords to access PHI.
- **ALL HEALTHCARE INFORMATION MUST BE PROTECTED AND TREATED AS CONFIDENTIAL.**

*Initial each to accept the Policy*

Initial	Policy
	1. It is the policy of Baptist 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 Baptist clinical site, Program Participants 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. Program Participants may not release or display copies of PHI.
	5. Program Participants 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 Program Participants. Program Participants are responsible and accountable for all work done under the associated access.
	7. Computer IDs or passwords may not be disclosed to anyone. Program Participants are prohibited from attempting to learn or use another person’s computer ID or password.
	8. Program Participants agree to follow Baptist’s privacy policies.
	9. Breach of patient confidentiality by disregarding the policies governing PHI is grounds for immediate dismissal from Baptist.

- I agree to abide by the above policies and other policies at Baptist’s facilities. I further agree to keep PHI confidential.
- I understand that failure to comply with these policies will result in disciplinary actions including dismissal from Baptist’s clinical facilities.
- 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



# BAPTIST HEALTH CARE CORPORATION

## Terms and Conditions for BHC Workforce Members Who Access BHC Confidential Information

**Workforce Members are:** Full and part-time employees, credentialed and employed physicians, volunteers, and students of BHC and/or its affiliates, and any employees or personnel of independent contractors of BHC and/or its affiliates working under the direct supervision of a BHC leader.

**By signing this form, I agree to the following Terms and Conditions in consideration of my employment with Baptist Health Care Corporation and/or one of its affiliates (hereinafter collectively referred to as "BHC"):**

**Legal and Ethical Responsibility** – BHC has a legal and ethical responsibility to safeguard the Protected Health Information (PHI), identifiable personal information, employee benefits, compensation and personnel information, trade secrets, and other proprietary business information it develops, generates, collects, maintains, and uses. For purposes of this agreement and underlying BHC policy, this information is collectively known as BHC Confidential Information. This agreement is part of BHC's comprehensive strategy for protecting Confidential Information and it covers Confidential Information in any form or medium including paper, digital, analog, magnetic, film, electronic and oral (spoken).

**Application of Federal Privacy Regulations:** I acknowledge that, enhanced enforcement provisions covering the wrongful acquisition or disclosure of a person's health information were authorized under the Recovery Act of 2009 and that I am personally subject to Federal and/or State criminal prosecution for intentionally violating the medical privacy of another person. I understand that intentionally accessing another person's medical information without proper authorization or a legitimate clinical or business need is considered a misdemeanor crime and is punishable by up to 1 year in prison and fines up to \$50,000. I understand that committing this offense under false pretenses is a felony and increases imprisonment up to 5 years with fines up to \$100,000, and that committing this offense with the intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm is a felony and increases imprisonment up to 10 years with fines up to \$250,000.

**System Monitoring and Auditing and No Expectation of Privacy**– I understand that BHC has the legal right and technical ability to monitor the use of all electronic systems owned or operated by BHC and that BHC can do this without any prior warning or notice. I understand that I have no expectation of privacy when using BHC information systems, desktops and laptops, tablet and other handheld devices, e-mail and texting solutions, or Internet connectivity even if the use is for personal reasons. Use of any BHC computer system constitutes consent to such monitoring.

**Protection and Privacy of BHC Confidential Information** – I understand that I must safeguard all BHC Confidential Information that I may access or come in contact with and that I must hold the information in strict confidence and not make any unauthorized disclosures of it and that my obligation to comply with the terms and conditions of this agreement shall continue even after I leave my employment and/or association with the BHC and/or its affiliates.

**Access to BHC Confidential Information** - I will not request, access, use, and/or disclose BHC Confidential Information for any purpose other than for the performance of authorized activities or duties. **I understand that I must follow established procedures for the authorized release of information to access information pertaining to my own care or the care of my spouse or children.** The only exception is when I am accessing this information in the course of my normally assigned duties and then only to the extent necessary to carry out those duties. When requesting or accessing BHC Confidential Information, I agree to request or access only the minimum amount of information necessary to accomplish my legitimate responsibilities. I will not allow others to access information unless my authorized activities require that I do so, and in such cases, I will only disclose or allow access to individuals having appropriate authorization and a legitimate business need to access the information.

**Information Systems Access User Identifiers (IDs), Passwords and Pass Codes** – I understand that I am responsible for any user IDs and passwords/codes provided to me by BHC. I understand that it is my responsibility to protect my passwords and codes and not share them with anyone. I understand that when authenticated by my password, my user ID will carry the same legal significance as my written signature. I further understand that I am responsible for any system activity that occurs under my user ID. I agree to immediately notify BHC in the event my password or pass code becomes compromised by calling the Information Services Help Desk at 1-800-642-3947. I understand that sharing my passwords or pass codes or intentionally circumventing BHC access controls may violate state or Federal laws and that BHC may inform appropriate authorities including professional licensing boards and agencies of my activities. These disclosures may identify me and contain detailed audit logs of any system activity that was conducted under my user IDs. I understand that BHC is not required to notify me before cooperating with authorities.

**BHC E-mail Systems and Internet Access** – If granted access to BHC e-mail systems and/or Internet access, I understand that any e-mail addresses assigned to me are BHC's property and represent BHC and that e-mail communications must be in accordance with established BHC policy. I further understand that it is my responsibility to become familiar with and abide by BHC policies and procedures governing the use of computers and electronic communication systems.

**Copying, Printing, Transmitting and Storing Confidential Information** – I understand that I am never authorized to remove Confidential Information from my BHC workspace or BHC computer systems unless doing so is part of my authorized duties and done in accordance with established policies and procedures. I understand that I am prohibited from copying, printing, downloading, e-mailing, texting, or otherwise electronically transmitting, duplicating or removing any BHC Confidential Information unless doing so is part of my authorized duties and done in accordance with established policies and procedures.

**Ownership of Data and Work Product** – I understand that any data and documents generated by me as a part of my duties while working for BHC is the property of BHC. This includes both Confidential Information and non-Confidential Information and applies to all information regardless of medium. I further understand that any work product created by me during my course of employment with BHC is the property of the corporation and that ownership and control of such work product will not transfer to me upon termination of employment unless expressly authorized by appropriate BHC officials.

**Unauthorized Software and Security Configuration Tampering** – I understand that I may not install any counterfeit, bootleg, unlicensed, or unauthorized programs or electronic content such as videos, music, eBooks, or other copyrighted materials on any BHC computer. I will not tamper with, alter, or disable any anti-malware software, firewall configurations or other settings, controls, or security features installed on any BHC device.

**Personal E-mail, Texting and Internet (Cloud) Based Services** – I understand that it is a violation of BHC policy and that I am never authorized to transmit BHC Confidential Information to or from a personal e-mail address or text account or to upload BHC Confidential Information to Cloud based services such as Dropbox, iCloud, Google Docs, Google Drive, Microsoft360 or similar services not provided by BHC.

**Electronic Portable Media** – I understand that personally owned media such as thumb drives, portable hard drives, flash memory devices, CD/DVD writers and similar devices may not be connected to BHC computers or the BHC network without first obtaining written authorization. In no event shall BHC Confidential information be placed on portable media that is not owned by BHC and fully encrypted to standards specified under Federal law.

**Personal Electronic Devices – Desktops, Laptops, Smartphones, Tablets, Pads, Smartpens, Cameras and Video/Audio Recorders** – I understand that any use of Personal Electronic Devices for BHC purposes must be in accordance with established policy and utilize only BHC approved software solutions that meet federal and state information security requirements. I understand that I may never place BHC Confidential Information on a personal device unless I am approved in writing to do so and I utilize BHC supplied secure applications.

**Personal Electronic Device Etiquette** – I understand that BHC leadership may restrict the use of personal electronic devices in the workplace to ensure the privacy and safety of patients and clients and to promote a positive work environment. I understand that I am expected to use good judgment and follow established policies while using these devices. I understand that I may never capture audio, video or photographic images of patients or clients or any part of their body including any wounds, tattoos, or other unique or identifying marks unless doing so is necessary to the treatment process. In any event, I may only use a BHC owned device or secure applications provided by BHC to capture or record such images, video or audio.

**Reporting of Information Security and Privacy Incidents** – An incident occurs when Confidential Information is obtained by, or disclosed to, an unauthorized person or entity or when controls protecting Confidential Information may have been compromised. I agree to immediately report information security and privacy incidents brought to my attention by notifying my supervisor or calling the BHC Information Services Help Desk at 1.800.642.3947, and reporting the incident in the STARS Enterprise Incident Reporting System.

**Anonymous Reporting (BHC Compliance Hotline)** – I understand that I may anonymously report incidents or violations of this agreement or any BHC policy by calling the BHC Compliance Hotline at 1.800.955.3998 or by making an on-line report at: <https://bhcgrc.alertline.com>.

<b>Last Name:</b>	<b>First Name:</b>	<b>MI</b>	<b>Preferred Name:</b>
<b>BHC/LCI Employee Number:</b>		<b>Facility:</b>	
<b>BHC Employee</b> <input type="checkbox"/> <b>or</b> <b>Workforce Member</b> <input type="checkbox"/>			
<b>Relationship to BHC</b>		<b>Company</b>	
<b>(Volunteer, student, contractor, consultant, temp, etc.)</b>		<b>(if applicable)</b>	
I have read this agreement and fully understand the conditions outlined above. I understand that access to BHC computer systems and Confidential Information is granted in order for me to perform my authorized job functions and that my access can be revoked at any time due to misuse or abuse. By signing below I agree to comply as stated. I further understand that inappropriate disclosure and/or access of Confidential Information or any breach of BHC confidentiality, privacy, and security policies will result in disciplinary action up to and including discharge and/or possible legal action or notification of authorities where appropriate. I understand and agree that my obligation to comply with the terms and conditions of this agreement shall continue even after I leave my employment and/or association with BHC and/or its affiliates.			
<b>Employee / Workforce Member Signature:</b>			<b>Date:</b>

**Retention: This is a legal document. In accordance with 45 CFR 164.530 (j) (1) (2), completed original or an electronic image thereof must be retained for 6 years from the date the applicant no longer has access to BHC Confidential Information.**