Bothwell™
Regional Health Center

Clinical Rotation Student Checklist

Documents that must be submitted to the Human Resources Office at least one week prior to clinical rotation:

- ✓ Completed Application
- ✓ Four Key Basics
- ✓ HIPAA Compliance
- ✓ Information Systems Access Agreement
- ✓ Confidentiality Statement
- ✓ Complete registration for MO Family Care Safety Registry (instructions below)

    - Log on to http://health.mo.gov/safety/fcsr/
    - Register Online
    - Registration
    - Register Online
    - Is A Person Registered
    - Social Security Number
    - Confirm Social Security Number
    - Confirm "I'm not a robot"
    - Search
    - Continue
    - Employer Name – Bothwell Regional Health Center
    - Select if No Employer – choose Student
    - Continue
    - Registration Type – Hospital
    - The remaining items are asking for your personal information

Requirements for the day your clinical rotation begins:

- ✓ Arrive at the Human Resources office 15 minutes prior to scheduled time
- ✓ Obtain ID badge from Human Resources
- ✓ Dress professional. Scrubs and clean comfortable tennis shoes may be worn in clinical areas. Business casual is required in all other departments. Jeans are not allowed.

Bothwell Regional Health Center Clinical Rotation Application

Applicant's Name_____

Date of Birth_____ Age_____ Social Security # _____

Street Address_____

City_____ State_____ Zip Code_____

Home Phone_____ Cell Phone_____

Email Address_____

Preferred Contact Method_____

School Attending_____

Program / Major_____

Current Grade Level_____

Parent / Legal Guardian (if minor)_____

Contact Phone Number_____

Emergency Contact_____

Emergency Contact Phone Number_____

Department / Unit requested _____

Total number of hours requested_____
(Please note that the number of hours is not guaranteed.)

First available date to job shadow (MM/DD/YYYY)_____

Please indicate below your availability for each day.

Monday_____Tuesday_____Wednesday_____Thursday_____Friday_____

Please describe your interest in job shadowing at Bothwell Regional Health Center.

_____

_____

Human Resources Department (660) 827-9540 tnappe@brhc.org

FOUR KEY BASICS

Safety

I practice safe behaviors to ensure the well-being of all.

Courtesy

I will be welcoming and available to visitors, patients and peers.

Professionalism

I choose to commit to my role at Bothwell with honor and integrity at all times.

Efficiency

I ensure our patients' needs are fulfilled in a timely, accurate and cost-effective manner.

Name (please print) _____

Employee ID _____

Signature _____

Date _____

Bothwell™
Regional Health Center

GET WELL. STAY WELL. BOTHWELL.

Document Number:	**Form HIPAA-1.A**	Page 4 of 6
Document Name: **Confidentiality Agreement of Workforce Member**		

I am a Workforce Member of Bothwell.

1. I understand the definition and meaning of the terms Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) and that while carrying out my duties and responsibilities as a Workforce Member I may create, receive, maintain or transmit PHI and EPHI and that PHI and EPHI may be disclosed to me or used and disclosed by me .
2. I understand that protection of the privacy and security of PHI and EPHI is a core value of Bothwell and the purpose of the Organization's HIPAA Compliance Program and that I must follow its HIPAA Compliance Program Policies and Procedures at all times.
3. I have received familiarization training about The HIPAA Compliance Program of Bothwell including training about the 6 Basic HIPAA Policies including the Minimum Necessary Standard, Prevention of a Breach of Unsecured PHI and a HIPAA Compliance Official who I can contact whenever I have a question or want more information about HIPAA.
4. In consideration for being a Workforce Member of Bothwell I agree to:
   A. Comply fully with the Organization's HIPAA Compliance Program;
   B. Use, disclose or request PHI and EPHI only as permitted by the Organization's HIPAA Compliance Program's Policies and Procedures; and
   C. Report any use, disclosure, acquisition or access of PHI or EPHI created, received, maintained or transmitted by or on behalf of Bothwell that violates, or I think may violate, a Policy or Procedure of the HIPAA Compliance Program by anyone including me, another Workforce Member of Bothwell or by any other person as soon as I become aware of it to a HIPAA Compliance Official.
5. I understand that if I violate a Policy or Procedure of the HIPAA Compliance Program of Bothwell I may be violating the law and may even be subject to criminal prosecution depending on the facts of the violation.
6. I understand that if I violate a Policy or Procedure of the HIPAA Compliance Program of Bothwell including the terms of this Confidentiality Agreement I may be subject to sanctions based on the nature of the violation including possible termination of my employment.
7. I understand and agree that my obligations under this Confidentiality Agreement to protect the privacy and security of PHI and EPHI shall survive the end of my association with Bothwell as a Workforce Member.

I have read and understand this Confidentiality Agreement and by placing my signature below confirm I will comply fully its terms and the HIPAA Compliance Program of Bothwell.

Workforce Member Signature	Printed Name	Date

Bothwell Regional Health Center

Information Systems Department
Access Agreement Form

I agree to the following conditions for any computing, network, email, and /or internet access services:

(1) I shall use any BRHC computer or network facility only with proper authorization. I shall not assist in, encourage, or conceal any unauthorized use or attempt at unauthorized use, of any BRHC computers or network facilities.

(2) I will not willfully interfere with others' authorized computer usage.

(3) I shall use BRHC communication facilities for job related work only, and will not use any BRHC computer or network facility for non-BRHC business.

(4) I understand no computer will be connected to any BRHC network unless it meets technical and security standards. Personally owned devices are not permitted on a BRHC network.

(5) I will not interfere with others' legitimate use of any computer or network facility.

(6) I shall not give any password for any BRHC computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means.

(7) I will not read, alter, or delete any other person's computer files or electronic mail without that person's permission.

(8) I shall not copy, install, or use any software or data files in violation of applicable copyrights or license agreements.

(9) I will not create, install, or knowingly distribute a computer virus, "Trojan Horse," or other surreptitiously destructive program on any BRHC computer or network facility.

(10) I will not install new software nor modify or reconfigure existing software or hardware of any BRHC computer or network facility.

(11) I recognize the email system is the property of BRHC, and all my messages are for business use and not considered personal or private.

(12) I am responsible for messages I transmit through BRHC computers and network facilities. I shall not use BRHC computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.

(13) I understand Internet access is "filtered", "monitored", and "logged". "Filtered" means access to sites deemed inappropriate by management is blocked. "Monitored" means the Information Systems department actively uses automated and manual methods for examining activity as well as content. "Logged" means all communications in our system generate an electronic trail. A record of the transaction is kept on file.

_____

STUDENT'S FULL ***LEGAL*** NAME

_____

STUDENT'S ***'GO BY'*** NAME

_____

STUDENT SIGNATURE

BOTHWELL REGIONAL HEALTH CENTER

Student
Confidentiality Statement

BHRC has adopted the following "Information Privacy, Confidentiality, Integrity and Security" policy as part of its overall <u>INFORMATION MANAGEMENT PLAN</u>:

The Hospital is responsible for protecting its information, including the access, the extent of access, the maintenance of confidentiality, the release and the security of information.

Each department, each employee and each member of the Medical Staff is obligated to keep all clinical information confidential, secure, complete and safe from physical damage. Each department shall be responsible for determining the need for different levels of security for different types of information, i.e.; clinical, personnel, payroll, financial or administrative.

PATIENT PRIVACY AND CONFIDENTIALITY: The patient has a right, within the law, to personal privacy and confidentiality, and to assume that all communications and all records pertaining to his of her care be confidentially treated and read only by individuals directly involved in his or her treatment or the monitoring of its quality.

<u>PROCEDURE:</u>

- **I.** **Each participant must sign a Confidentiality Agreement (as listed below) covering his/her obligation to maintain this policy as outlined above.**
- **II.** **Each Department will develop a confidentiality plan that meets that department's obligation for maintaining this policy.**

= =

<u>Confidentiality Agreement</u>

I understand and agree that in the performance of my duties as the undersigned , I must hold all medical information in confidence. I also understand that I should only have access to information necessary to observe in the area of my health career interest, and that I have an obligation to keep confidential any information to which I have access. This includes clinical, personnel, payroll, financial, or administrative information. I understand that any violation of the confidentiality of such information (even to my spouse or family member) may result in disciplinary action by the entity I represent, and may subject me to criminal and/or civil charges and penalties under Missouri state statutes as well as Federal law (HIPAA).

This confidentiality agreement applies equally to any electronic information as well, and that unauthorized use or access of any employee's password may result in punitive action.

Date:	Signature: x	Print Name: