

Administrative
 Departmental

SUBMITTED BY: Adriene McCoy **APPROVED BY:** Corey B. Heller
Adriene McCoy Corey B. Heller
Title: Assistant Vice President, Human Resources **Title:** Corporate Vice President and Chief Human Resources Officer
Responsible Department: Human Resources

Creation Date: 08/20/02
Review Date: 03/20/04, 11/01/10
Revision Date: 11/01/08, 11/01/10

POLICY TITLE:
Unauthorized Release of Confidential Information

SUMMARY & PURPOSE:

To establish an system-wide philosophy and policy to protect and preserve the privacy and confidentiality of employee and patient protected medical information, as well as, proprietary, trade secret, personal, privileged or otherwise sensitive data and information collectively, "Confidential Information."

POLICY:

Employees, contractors and volunteers of Baptist Health are prohibited from using or disclosing Confidential Information (as defined in this Policy) for any purpose other than to conduct the business of Baptist Health. Employees, contractors and volunteers shall not disclose, share, copy, or transmit Confidential Information to anyone who is not authorized to receive it, or otherwise violate the confidentiality of such data or information. At all times, all employees are expected to protect the integrity, security and confidentiality of Confidential Information to which they may have access or with which they come in contact.

SCOPE/APPLICABILITY:

Applies to all Baptist Health South Florida employees, contractors, and volunteers, both during the course of their employment/relationship with Baptist Health, and after the termination of their employment/relationship with Baptist Health.

PROCEDURES TO ENSURE COMPLIANCE:

1. Definitions:

- a. Confidential Information: Confidential Information includes, but is not limited to, information regarding patients, contractual relationships with third party payors and others, the medical staff, and information regarding the Company and its affiliates' business, affairs, plans, employees, methods and systems, trade secrets and

All references to Policies must go to the BHSF Master Copy on the BHSF Intranet; do not rely on other versions / copies of the Policy.

management philosophy relating to Baptist Health of its affiliates' business practices for corporate purposes only. Examples of Confidential Information include:

- i. Employee and Patient account and billing information, including but not limited to Social Security Numbers.
 - ii. Employee and Patient medical information and records.
 - iii. Patient and customer lists.
 - iv. Individual rates of pay.
 - v. Corporate financial long and short range strategies.
 - vi. Financial information.
 - vii. Payroll information.
 - viii. Productivity measures.
 - ix. Short and long range staffing plans.
 - x. Managed care contract strategy and information.
 - xi. Computer software and data ideas.
 - xii. Magnetic, image and text electronic information.
 - xiii. Trade secrets.
 - xiv. Marketing and advertising methods.
 - xv. Personal employee information, including but not limited addresses, telephone numbers, credit/debit card information, bank account information, benefit information, and Social Security Numbers.
 - xvi. Network ID's and passwords.
- b. Patient Information and Records:
In order to protect patient information from inappropriate disclosure, employees are expected to:
- i. Limit their access to patient information to that required by their duties, permitted by law and authorized by Baptist Health;
 - ii. Use only legitimate and authorized means to collect patient information and, whenever practical, obtain it directly from the patient;
 - iii. Not release information concerning patients in drug and alcohol treatment programs and information regarding a patient's HIV status unless permitted to do so by laws and regulations which apply to this information;
 - iv. Refrain from revealing any patient information unless supported by legitimate business or patient care purposes; as defined by Baptist Health;
 - v. Not discuss health information about a patient with any person inside or outside Baptist Health unless it is in connection with an employee's work, is permitted by law and is authorized by Baptist Health;
 - vi. Exercise discretion when discussing patient information by being aware of the work area surroundings and guarding against visitors and third parties needlessly overhearing patient health information; and
 - vii. Refrain from removing or retrieving a patient medical record, or a copy of such record, from a designated storage facility or department without the authorization of a leader or other designated official.
 - viii. Refrain from accessing confidential information for personal use or gain.
- c. Business Records:
All business records of Baptist Health are proprietary and confidential. Therefore, employees will limit their access, use and disclosure of business information and business records to that required for employees to perform duties as an employee of Baptist Health. Employees will not remove business or corporate records, or copies of such records, from any department without authorization of the department leader.

2. Procedure:

- a. All employees are required to sign the Confidentiality and Non-Disclosure Agreement (Attachment A) at the time of hire or at the time of issue of this policy.

- b. Leaders are responsible for ensuring that employees understand Baptist Health's confidentiality policy. The policy and expectations should be discussed regularly in staff meetings.
- c. If an employee becomes aware of a violation of this policy, he/she must report the incident immediately to the department leader or the Chief Privacy Officer or may anonymously report to the HIPAA Hotline at 786-596-8850.

SUPPORTING/REFERENCE DOCUMENTATION:

- N/A

RELATED PROCEDURES AND ASSOCIATED FORMS:

- Attachment A: Confidentiality and Non-Disclosure Agreement

ENFORCEMENT & SANCTIONS:

Violation of this policy may lead to disciplinary action, up to and including termination of employment.