Baptist Health South Florida

POLICY NO.: BHSF-5225
TYPE: Administrative

POLICY TITLE: Unauthorized Release of Confidential Information

Responsible Department: Human Resources

Creation Date: 08/20/2002
Review Date:
Revision Date: 2/28/2023 12:00:00 AM

SUBMITTED BY (AUTHOR): Carrie Bustos
Title: Director, Employee Relations

APPROVED BY: Mercedes del Rey
Title: Assistant Vice President, Chief Privacy Officer

APPROVED BY: Claudia Swaby
Title: Assistant Vice President, Human Resources

APPROVED BY: Philip Magin
Title: Vice President, Human Resources

APPROVED BY: Adriene McCoy
Title: Senior Vice President and Chief People Officer

PUBLISHED (Released): Tuesday, March 28, 2023 8:00:00 AM

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

POLICY:
Baptist Health South Florida, Inc. ("BHSF" or "Baptist Health") has a longstanding commitment to maintaining the highest standards of clinical and service excellence. As part of that commitment, we recognize the importance of maintaining and protecting the privacy of our employee, financial and patient information in every aspect of the care and services we provide. 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 Baptist Health business. Employees, volunteers, trainees, students, temporary staff, and contractors/consultants shall not disclose, share, copy, or transmit confidential information to anyone who is not authorized to receive it, store confidential information (electronic or paper), or otherwise violate the confidentiality of such data or information. At all times, everyone subject to this policy must protect the confidentiality, integrity and security of Baptist Health confidential information to which they may have access or with which they come in contact.

SCOPE/APPLICABILITY:
This policy applies to all Baptist Health South Florida employees, volunteers, trainees, students*, temporary staff, and contractors/consultants both during and after their employment/relationship with Baptist Health South Florida. ***Students.** Employed students are treated as employees. Non-employed students (including fellows, residents, students) must comply with this policy pursuant to the terms of their applicable academic agreements.

Definitions:

1. Confidential Information: Confidential information includes, but is not limited to information regarding patients, contractual relationships with third party payers and others, medical staff, information regarding Baptist Health and its affiliates' business, affairs, plans, employees, methods and systems, trade secrets and management philosophy.

2. Confidential **Patient** Information (Protected Health Information (PHI)) includes:
   a. Patient account/billing information, social security numbers, medical records and/or any medical information related to the care and treatment of a patient; or
   b. Protected Health Information (PHI), which is information that:
      i. Relates to an individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and
      ii. Either identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual; and
      iii. Exists in oral, written, and electronic formats.

3. Confidential **Baptist Health Business** Information includes:
   a. Any employee information contained in an employee's Human Resources, Departmental, Occupational Health Office or any other type of employment file maintained by Baptist Health, including personal employee information such as addresses, telephone numbers, credit/debit card information, bank account information, benefit information (including but not limited to health/insurance policy, Medicare, Medicaid and or Veterans Administration numbers), Driver's License numbers, Passport/Visa and Social Security Numbers;
   b. Patient, customer or vendor lists;
   c. Corporate financial long and short range strategies;
   d. Financial information;
   e. Payroll records;
   f. Productivity measures;
   g. Short and long range staffing plans;
   h. Managed care contract strategy and information;
   i. Computer software and data ideas;
   j. Magnetic, image and text electronic information;
   k. Trade secrets;
   l. Marketing and advertising methods; or
   m. Network ID's and passwords.

4. Personally Identifiable Information (PII): information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PROCEDURES TO ENSURE COMPLIANCE:

1. Employee Information and Records: In order to protect employee information from inappropriate access, use and disclosure, employee files (including but not limited to Human Resources, Departmental, and Occupational Health Office files) and employee information must be maintained in a secure location. All workstations must be locked when not in use.

2. Patient Information and Records: In order to protect patient information from inappropriate access, use and disclosure, everyone subject to this policy must:
   a. Limit their access to patient information to that required by their duties, permitted by law and authorized by Baptist Health;
   b. Use only legitimate and authorized means to collect patient information and, whenever practical, obtain it directly from the patient;

c. 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;
d. Refrain from revealing any patient information unless supported by legitimate business or patient care purposes, as defined by Baptist Health;
e. 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;
f. 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;
g. 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;
h. Refrain from accessing confidential information for personal use or gain;
i. Refrain from storing, disclosing or transmitting electronically any ePHI or electronic patient information, pictures of patients or patient information on personal mobile devices, cloud storage, laptops, cell phone, iPad, USB storage, cloud storage or personal email;
j. Refrain from storing, saving or removing from the facility any paper protected health information without prior authorization. This includes schedules, logs, work product, work examples, or any other patient information; and
k. Refrain from taking photos of patients or of patient information or sharing any patient information, including patient pictures, comments or descriptions of patients or patient interactions using social media or mobile devices, including text messages, tweets, posts or any other method of sharing patient information electronically. Reference policy BHSF-6750 Social Media and BHSF-6400 Electronic Devices at the Workplace.

3. Business Records: All business records of Baptist Health South Florida are proprietary and confidential. Therefore, access, use and disclosure of business information and business records must be limited to access required for employees to perform duties as an employee of Baptist Health. Employees are prohibited from removing business or corporate records, or copies of such records, from any Baptist Health department without authorization of the department leader.
   a. Everyone subject to this policy must respect and maintain the confidential/proprietary nature of confidential Baptist Health business information and/or confidential Personally Identifiable Information (PII), Patient Information, and Protected Health Information (PHI).
   b. Everyone subject to this policy is prohibited from the unauthorized use of, copying of, retention of or forwarding through electronic mail or social media (Facebook, Snapchat, Instagram, Twitter, LinkedIn, etc.) to third parties (including the employee's personal email and/or social media accounts) of Baptist Health official records and documents containing private, confidential or proprietary information regarding Baptist Health, its employees, patients, contractors, vendors, physicians, scholars, volunteers and/or vendors.
   c. Everyone subject to this policy is prohibited from unauthorized printing, copying of or saving onto external hard drives, USB drives or personal laptops all confidential Baptist Health business information regarding Baptist Health, its employees, contractors, physicians, scholars, volunteers and/or vendors, Personally Identifiable Information (PII), confidential Patient Information and Protected Health Information (PHI).

4. Procedure:
   a. All employees are required to sign the Confidentiality and Non-Disclosure Agreement (Attachment A) at the time of hire and annually during Annual Required Education (ARE).
   b. Leaders are responsible for ensuring that employees understand and adhere to Baptist Health's confidentiality policy.
   c. If anyone covered by this policy becomes aware of a violation of this policy, they must report the incident immediately to their department leader, Human Resources, Corporate Compliance or the Chief Privacy Officer and/or may report to the HIPAA Hotline at 786-596-8850 or Privacy@Baptisthealth.net.
   d. Failure to adhere to the guidelines described within this policy may subject the employee to corrective disciplinary action, up to and including termination of employment.

SUPPORTING/REFERENCE DOCUMENTATION:

- Health Insurance Portability and Accountability Act of 1996 as amended from time to time and including any regulations promulgated there under (collectively, "HIPAA")
- Florida Statute §501.171 ("Security of Confidential Personal Information")
- Applicable local, state and federal laws and regulations.

RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:

- BHSF Administrative Policies – Human Resources
  - 1150 Independent Contractors
  - 5225 Attachment A: Confidentiality and Non-Disclosure Agreement
  - 5250 Employee Conduct
  - 5270 Workplace Gossip
  - 5300 Corrective Action Policy
  - 6400 Electronic Devices at the Workplace
  - 6750 Social Media
- BHSF Administrative Policies – Corporate Privacy
  - BHSF-74220-001.00 – Unified Corporate Privacy Policy on HIPAA Compliance
  - BHSF-74220-202.00 – Safeguards - Safeguards for Verbal Written and Electronic Patient Information
  - BHSF-74220-301.00 – Use & Disclosure - Using, Disclosing and Requesting Patient Information for Baptist Health Treatment Activities
  - BHSF-74220-605.20 – Compliance and Implementation – Sanctions for Privacy Violations
  - BHSF-74220-701.00 – Privacy and Security Incident Reporting and Response
- BHSF Administrative Policies – Technology & Digital
  - BHSF-70491-104 - Acceptable Use of Computer, Email and Messaging
  - BHSF-70491-159 - Unified Corporate Policy for Compliance with the HIPAA Security Rule
  - BHSF-70491-173 - Data Classification

ENFORCEMENT & SANCTIONS:

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

1. Reference: HIPAA Privacy Policy BHSF-74220-605.20 – Sanctions for Privacy Violations.
2. Violations of this policy will be determined by the Chief Privacy Officer in consultation with Baptist Health Administration and the appropriate Human Resources management level. Reference: HR policies 5250 and 5300.
3. Violations of this policy may lead to disciplinary action up to and including termination.
4. Enforcement of this policy will be performed by Human Resources and/or the Baptist Health South Florida Privacy Office.