



POLICY TITLE: 301.00 Accessing, Using, Disclosing or Requesting Patient Information for Baptist Health Treatment Purposes

Responsible Department: Corporate Privacy Office

Creation Date: 04/07/2003

Review Date: 2021/12/13

Revision Date: 2021/12/13

SUBMITTED BY (AUTHOR): Mercedes del Rey

Title: Assistant Vice President, Chief Privacy Officer

APPROVED BY: Janette Sanchez

Title: Vice President, Finance

APPROVED BY: Matthew Arsenault

Title: Executive Vice President & Chief Financial Officer

PUBLISHED (Released): 2021/12/13

SUMMARY & PURPOSE:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a Baptist Health or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule sets out how and with whom PHI may be shared.

POLICY:

It is the policy of Baptist Health South Florida, Inc. ("BHSF" or "Baptist Health") to comply with applicable state and federal laws, including those protecting the confidentiality of patient health information and establishing certain individual privacy rights. It is our policy to implement these laws in a way that supports our primary mission to the community regarding the delivery of quality health care in an efficient manner.

This policy governs accessing, using, disclosing or requesting patient information for Baptist Health treatment purposes.

SCOPE/APPLICABILITY:

This policy applies to Baptist Health, its affiliates, all workforce members, and others as described below.

- **Workforce members.** Workforce members means employees, volunteers, trainees, temporary staff, and contractors/consultants who are not independent contractors under *Human Resources Policy 1150 - Independent Contractors*.
- **Medical staff members.** Medical staff members are treated as members of an organized health care arrangement with Baptist Health South Florida and must comply with this policy as if they are workforce members pursuant to their applicable medical staff bylaws.

- **Students.** Employed students are treated as workforce members. Non-employed students (fellows, residents, students) must comply with this policy as if they are workforce members pursuant to the terms of their applicable academic agreements.
- **Independent Contractors and Others.** Independent Contractors and others who have agreed to comply with Baptist Health's policies and procedures as a condition of receiving access to Protected Health Information (PHI) must comply with this policy as if they are workforce members.

DEFINITIONS:

1. Protected Health Information:
 - a. Information that 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
 - b. Either identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual; and
 - c. Exists in Oral, Written, and Electronic Formats.

PROCEDURES TO ENSURE COMPLIANCE:

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 patients in every aspect of the care and services we provide.

1. Privacy and Confidentiality at Baptist Health is one of our service excellence standards. As individuals involved in the delivery of health care, anyone covered by this policy must:
 - a. Safeguard protected health information as part of their job at Baptist Health.
 - b. Be responsible for maintaining protected health information confidential, and only use it for treatment, payment and health care operations as set forth in the Privacy Rule.
2. Quality Treatment is the Primary Objective
 - a. Anyone covered by this policy may use, disclose and request whatever information about a patient when it is necessary to treat or provide health care services to the patient, or arrange for treatment.
 - b. Ethical and professional standards assuring the provision of quality health care and the immediate physical, social and psychological needs of a patient are the primary concern in deciding how to use or disclose patient information.
 - c. Subject to this primary concern, every individual covered by this policy must:
 - i. Make reasonable efforts to limit the patient information used to the minimum amount necessary to accomplish the intended purpose
 - ii. Shall be mindful of the identification credentials of persons who are present in the immediate setting where a patient's care is discussed; and
 - iii. Shall take reasonable steps to assure that incidental disclosures to bystanders (including clergy, vendors, visitors and any unidentified persons who may be present) are consistent with professional ethical standards for balancing the patient's health care and privacy interests.
 - d. It is never reasonable to limit information if doing so might influence an action or decision that could adversely affect the patient's health care or well-being.
3. Using Patient Information for Treatment
 - a. Health care professionals and medical staff members that provide treatment to Baptist Health patients shall have access at all times, to ensure quality care, to the entire paper and electronic medical record of a patient to whom they currently are rendering treatment or for whom they are providing a consultation or second opinion.
 - b. Physicians who did not participate in the care of the patient for a particular admission/registration and are currently treating the patient, or physicians treating a patient admitted/registered to one of the system's hospitals, are entitled to copies of requested health information by providing patient

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.

- authorization, completing a staff physician request form, or providing a written request stating they are currently treating the patient on their letterhead.
4. Requests for patient information from other health care providers
 - a. Individuals who are covered by this policy and whose duties require them to request patient information from other health care providers or health plans for treatment purposes may request such information for the treatment of a Baptist Health patient.
 5. Disclosures of patient information
 - a. Individuals who are covered by this policy may disclose patient information to another health care provider (or the staff of another health care provider) for purposes of Baptist Health's treatment activities and for treatment in a physician office setting including, but not limited to, for consultation with the health care provider or for discharge planning.
 6. Accessing Patient Information
 - a. Individuals covered by this policy may not access, use or disclose BHSF patient information, paper or electronic, for a patient for whom they have not been assigned patient care responsibilities.
 - b. Anyone covered by this policy may not access patient information in any form or format unless it pertains to their role at Baptist Health.
 - c. PHI may only be accessed, used, or disclosed for treatment, payment, or health care operations and the access may not compromise the confidentiality, availability or integrity of the PHI.
 - d. Anyone covered by this policy may never:
 - i. Use their BHSF computer access to "look up" information about a patient for personal or non-job related reasons.
 - ii. Use their authorized access to BHSF computer systems to review family or friends' protected information despite having no business purpose to do so.
 - iii. Access the paper medical record of a patient for personal or non-job related reasons.
 - iv. Access PHI to review information about co-workers, friends, or family members out of curiosity, i.e., without a medical or business-related purpose.
 - v. Remove any patient information (electronic or paper) from the department for unauthorized reasons.
 - vi. Verbally share a patient's information to an unauthorized third party.
 - vii. Discuss a patient's PHI in an unauthorized public area such as the elevator, cafeteria, or outside of work or for or business-related purposes.
 7. Deceased individuals
 - a. Baptist Health must comply with the requirements of this policy with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

SUPPORTING/REFERENCE DOCUMENTATION:

- Health Insurance Portability and Accountability Act of 1996 as amended from time to time and including any regulations promulgated thereunder (collectively, "HIPAA")
- Applicable Florida State Laws

RELATED POLICIES, PROCEDURES AND ASSOCIATED FORMS:

- Corporate HIPAA Privacy Policies
- 10000-74220-001.00 Unified Corporate Privacy Policy on HIPAA Compliance
- HIM 400 Use or Disclosure of Medical Record Information

ENFORCEMENT & SANCTIONS:

1. Reference: Corporate HIPAA Privacy Policy 10000-74220-605.20 Sanctions for Privacy Violations

2. Violations of this policy will be determined by the Chief Privacy Officer in consultation with the appropriate levels of department leadership and appropriate Human Resources management level. Reference: HR policies 5250 Employee Conduct and 5300 Corrective Action.
3. Violations of this policy may lead to disciplinary action up to and including termination.
4. Enforcement of this policy will be performed by Baptist Health South Florida's Privacy Office in conjunction with Human Resources, as circumstances may dictate.