



**POLICY TITLE:** 303.00 Uses and disclosure of Health Information for Healthcare Operations and Administrative Purposes

**Responsible Department:** Corporate Privacy Office

**Creation Date:** 04/07/2003

**Review Date:** 2021/12/15

**Revision Date:** 2021/12/15

**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):** 2021/12/20

---

## **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 administrative activities.

## **SCOPE/APPLICABILITY:**

This policy applies to Baptist Health, its affiliates, all workforce members, and others as described below that use disclose or request patient information for Baptist Health's administrative operations.

- **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.

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.

- **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. Health Care Operations: Any of the following administrative activities of Baptist Health to the extent that the activities are related to covered functions:
  - a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
  - b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - c. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - d. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
  - e. Business management and general administrative activities of Baptist Health, including, but not limited to:
    - i. Management activities relating to implementation of and compliance with the requirements of the Privacy Rule;
    - ii. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;
    - iii. Resolution of internal grievances;
    - iv. The sale, transfer, merger, or consolidation of all or part of Baptist Health with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
    - v. Fundraising for the benefit of the covered entity.
2. Protected Health Information:
  - a. Information that relates to the 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:**

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.

Baptist Health may use and disclose health information for healthcare operations and administrative purposes. These uses and disclosures are necessary to make sure that all of our patients receive quality care and for Baptist Health operation and management purposes. For example, Baptist Health may use health information to review the treatment and services we provide to ensure that the care our patients receive is of the highest quality, or we may post in employee areas thank-you notes or pictures that patients send us.

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 using it for treatment, payment and health care operations as set forth in the Privacy Rule.
2. Permissible Baptist Health Administrative Activities.
  - a. Baptist Health may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if
    - i. Each entity either has or had a relationship with the individual who is the subject of the protected health information being requested; or
    - ii. The protected health information pertains to such relationship, and the disclosure is:
      - 1) For a purpose listed in the definition of health care operations; or
      - 2) For the purpose of health care fraud and abuse detection or compliance.
  - b. Baptist Health may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.
3. Use of patient information for Administrative Activities
  - a. Access
    - i. Department leaders shall assume responsibility for determining whether an individual under their supervision has a job-related need to access patient information and the extent of access required by each individual.
    - ii. The leader of each individual covered by this policy and involved in Baptist Health administrative activities shall select the level of access for each person they supervise when authorizing credentials for accessing electronic medical records and requesting an identification badge.
  - b. Use of Entire Medical Record
    - i. When actively working on administrative activities with respect to a specific patient, access to the entire medical record may be necessary.
  - c. Time and Extent of Access
    - i. No employee or contractor involved in administrative activities shall have access to patient information other than during the specific hours that the individual is working on the specific account.
    - ii. No surplus copies of information or work papers shall be maintained.
    - iii. Each employee and contractor may access only the patient information for which their supervisor has approved access.
  - d. Documentation
    - i. Employees and contractors involved in administrative activities shall strictly follow departmental documentation and document retention policies.
4. Disclosure of and Request for Patient Information
  - a. Anyone covered by this policy that desires to have a third party pool and aggregate patient information with that of other providers for purposes of Baptist Health's administrative activities shall ensure that a Business Associate Agreement is executed in accordance with the applicable HIPAA Privacy Policy; and
  - b. Who May Disclose or Request Information
    - i. Supervisors shall ensure that before providing protected health information to third parties who agrees to perform analyses that may be useful for Baptist Health's administrative activities, including but not limited to outcomes analysis, benchmarking, cost and utilization studies, business administration the supervisor shall either execute a Data Use Agreement or have the data elements approved by the Corporate Privacy Office.

- ii. Department supervisors shall determine and document which employees and contractors are authorized to disclose information to, and request information from, health plans or others for Baptist Health administrative activities, whether by telephone, fax, email, mail or electronic data transmission.
  - c. Information Subject to Enhanced Privacy Protection
    - i. No individual covered by this policy may transmit or disclose any information that is subject to enhanced privacy protection to a health plan, or other person or entity for administrative purposes.
5. Minimum Necessary
  - a. When using, disclosing or requesting patient information for administrative activities of a Baptist Health facility, reasonable efforts shall be made to limit the patient information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
  - b. Anyone covered by this policy that is involved in administrative activities for Baptist Health shall use, disclose and request the minimum amount of patient information necessary for such payment purposes.
  - c. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, Baptist Health and its business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
  - d. Baptist Health must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purpose.
  - e. These minimum necessary policies and procedures also must limit who within the entity has access to protected health information, and under what conditions, based on the job responsibilities and the nature of the business.
  - f. BHSF Employees may only access, use and share as much information as is necessary for accomplishing the intended purpose.
6. 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
- BHSF-74220-001.00 Unified Corporate Privacy Policy on HIPAA Compliance
- HIM 400 Use or Disclosure of Medical Record Information
- Attachment - BHSF HIM 6001 Authorization for Release of Health Information
- Attachment - BHSF HIM 6001 Authorization for Release of Health Information (Spanish)

**ENFORCEMENT & SANCTIONS:**

1. Reference: Corporate 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 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.