POLICY TITLE: 302.00 Payment Activities - Using Disclosing and Requesting Patient Information for Baptist Health Payment Activities

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): 2021/12/15

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 payment 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 in the course of their duties at a Baptist Health facility or activities related to their office treatment to obtain payment from patients, health plans, and others for services rendered by Baptist Health.

- **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 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:

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 using it for treatment, payment and health care operations as set forth in the Privacy Rule.
2. Baptist Health may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
3. Anyone covered by this policy that is involved in payment activities for Baptist Health shall use, disclose and request the minimum amount of patient information necessary for such payment purposes.
4. Use of patient information for billing activities
   a. Access
      i. Personnel involved in payment activities include employees and contractors that are involved in medical coding, claims preparation, eligibility verification, prior authorization and payment reconciliation.
      ii. Department supervisors 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.
   b. Credentials and Badges
      i. The supervisor of each individual covered by this procedure and involved in Baptist Health payment 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.
   c. Use of Entire Medical Record
      i. When actively working on payment issues with respect to a specific account, access to the entire medical record may be necessary to ensure appropriate and accurate billing or prior authorization.
   d. Time and Extent of Access

i. No employee or contractor involved in payment 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 once a claim has closed.
iii. Each employee and contractor may access only the patient information for which their supervisor has approved access.

e. Documentation
i. Employees and contractors involved in payment activities shall strictly follow departmental documentation and document retention policies.

5. Disclosure of and Request for Patient Information
a. Who May Disclose or Request Information.
i. 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 payment activities, whether by telephone, fax, email, mail or electronic data transmission.
b. Information Subject to Enhanced Privacy Protection
i. No employee, volunteer, or contractor may transmit or disclose any information that is subject to enhanced privacy protection to a health plan, or other person or entity for payment purposes.
ii. When information is marked as being restricted, anyone covered by this policy shall consult the Corporate Privacy Office prior to any disclosure of the information. The Corporate Privacy Office shall notify each designated record set custodian of all granted enhanced privacy requests.
c. Minimum Necessary
i. 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.
1) 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.
2) These minimum necessary polices 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.
3) BHSF Employees may only access, use and share as much information as is necessary for accomplishing the intended purpose.
ii. When preparing a standard transaction, including but not limited to a claim for payment, eligibility check, or claims status check, the inclusion of data elements that are required for electronic transactions under the HIPAA transactions rule and those optional elements that are required by a health plan or under its trading partner agreement as a condition of payment shall be considered the minimum necessary information.

6. Requesting from and Responding to Requests from Health Plans or Physician Billing Services
a. Minimum necessary requests for protected health information.
i. Requesting: Baptist Health must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.
ii. Responding: When responding to billing related requests from health plans or physician billing services/personnel by fax, telephone, email, mail or electronic data request, each employee or contractor authorized by their supervisor to disclose patient information to health plans shall:
1) Verify that the information requested relates to services or procedures for which Baptist Health has sought payment from the health plan. All users will access information in accordance with the BHSF Safeguards Form; and
2) Not send the entire medical record, even when it is requested, unless specifically approved by the employee's or contractor's supervisor.
b. When a health plan or physician billing service/employee requests an attachment of a medical record or any portion of the record, or inclusion of a data element that is not part of the maximum data set promulgated under the HIPAA transactions rule, the request shall be sent to the patient financial services

or medical records department supervisor for evaluation of whether the information is the minimum necessary for the plan to make its determination.

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
- 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 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.