POLICY TITLE: 602.10 Compliance and Implementation - Privacy Training of BHSF Workforce

Responsible Department: Corporate Privacy Office

Creation Date: 04/07/2003
Review Date: 2021/12/14
Revision Date: 2021/12/14

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. It is the policy of Baptist Health to comply with applicable state and federal laws, including those protecting the confidentiality of patient health information and ensuring that its workforce is effectively trained to do so.

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 the privacy training of Baptist Health South Florida workforce members.

SCOPE/APPLICABILITY:
This policy applies to Baptist Health, its affiliates, all workforce members, and others as described below and all Baptist Health personnel charged with implementing the federal privacy regulations under HIPAA, including the Chief Privacy Officer and the Human Resources Department of each Baptist Health facility.

- **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.

PROCEDURES TO ENSURE COMPLIANCE:

Baptist Health must train all workforce members and individuals covered by this policy on the policies and procedures with respect to protected health information required by the Privacy Rule, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

1. The Chief Privacy Officer, in conjunction with the appropriate department, shall develop or procure training materials on Privacy Policies that are specific to the needs of the Baptist Health workforce.
2. Training
    a. On an ongoing basis, all members of the Baptist Health workforce shall be trained using the training materials developed in Section 1, as necessary and appropriate for members of the Baptist Health workforce to carry out their functions within the Baptist Health facilities.
    b. Such training shall include information on how to access the Privacy Policies and who to contact with questions about them.
    c. This training shall be provided prior to the compliance date during new workforce orientation:
        i. To each current Baptist Health workforce member, medical staff member, student, independent contractor or other r by no later than April 14, 2003; or September 23, 2013 for HIPAA Omnibus Regulations;
        ii. Thereafter, to each new member of the workforce and individuals covered by this policy within a reasonable period of time after the person joins Baptist Health;
        iii. To existing members of the workforce, or anyone covered by this policy, whose changed job assignment warrants a different level or type of privacy training; and
        iv. To each member of the workforce or anyone covered by this policy whose functions are affected by a material change in the HIPAA privacy policies and procedures, within a reasonable period of time after the material change becomes effective.
3. As necessary or appropriate, the Chief Privacy Officer may request or require additional training or retaining for any individual or group.
4. The Patient Experience department of each Baptist Health facility shall, at the request of the Chief Privacy Officer, assist in HIPAA awareness and training programs for the ancillary personnel who visit Baptist Health facilities, such as clergy, gift delivery firms and the like.
5. Human Resources and the Medical Staff Offices, at the request of the Chief Privacy Officer, shall:
    a. Ensure that privacy training is included in the orientation of all new Baptist Health employees, and other individuals covered by this policy;
    b. Document that the training has been provided and forward this documentation to the appropriate department for retention under the applicable HIPAA privacy procedure;
    c. Maintain a log of training and HIPAA awareness activities in each Baptist Health facility and forward this information as requested to the Corporate Privacy Office for retention under the applicable HIPAA privacy procedure; and
    d. Obtain a signed document indicating that the employee has received and understands the policies regarding client rights and confidentiality and retain the signed document in each employee's personnel record.

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:

- 10000-74220-001.00 Unified Corporate Privacy Policy on HIPAA Compliance
- 10000-74220-600.00 Compliance and Implementation – General Rule Regarding Privacy Compliance and Implementation
- Human Resources 5225 Unauthorized Release of Confidential Information
- Human Resources Attachment - Confidentiality and Non-Disclosure Agreement
- Human Resources 5250 Employee Conduct

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