POLICY TITLE: 702.00 Baptist Health South Florida Identity Protection Committee

Responsible Department: Corporate Privacy Office

Creation Date: 04/23/2009
Review Date: 2021/12/10
Revision Date: 2021/12/10

SUBMITTED BY (AUTHOR): Mercedes del Rey
Title: Assistant Vice President, Chief Privacy Officer

APPROVED BY: Karen Godfrey
Title: Corporate Vice President, Revenue Cycle Management

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.

In compliance with state and federal laws Baptist Health has developed an Identity Protection Program (the "Program") to assist BHSF in the detection, prevention and mitigation of identity theft that may occur with respect to certain accounts of patients that are created and maintained by BHSF. The Program will function in coordination with other efforts of BHSF to secure PHI in accordance with the HIPAA and other applicable federal and state laws.

The BHSF Board, or appropriate board level committee, must approve the program and thereafter be involved directly, or through a designated senior management employee, in the oversight, development, implementation and administration of the program. In addition, BHSF must assign specific responsibility for implementation, staff training, audit compliance, generate annual reports and oversee anyone granted access to covered accounts. BHSF is also required to update the program periodically to reflect changing risks to patients or the safety of BHSF from identity theft and medical identity theft. Alerts from law enforcement and others, changes in the methods of identity theft, changes in the methods to detect and prevent identity theft and changes to the infrastructure should be taken into consideration.

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. Baptist Health South Florida

delegates the administration of the Identity Protection Program ("Program Manager") to the Identity Protection Committee ("The Committee"). It is the duty of the Committee to serve as the Program Manager to define the Program and oversee the implementation and administration of the Program.

SCOPE/APPLICABILITY:

1. This policy applies to Baptist Health personnel charged with implementing the BHSF Identity Protection Program ("The Program"). The Program will be administered by the Identity Protection Committee.
2. The Identity Protection Committee will be composed of designated BHSF leaders who will provide the expertise from their respective departments and disciplines to ensure a sound and effective Program. The committee will include at least one representative from each of the following BHSF departments and will be chaired by the Chief Privacy Officer:
    a. Admitting and Registration
    b. Audit and Compliance
    c. Health Information Management
    d. Human Resources
    e. Information Technology
    f. Office of General Counsel
    g. Patient Financial Services
    h. Corporate Privacy Office
    i. Revenue Cycle Management
    j. Other departments as deemed necessary by the Committee

PROCEDURES TO ENSURE COMPLIANCE:

1. Baptist Health will convene the Identity Protection Committee to serve in the capacity of Program Manager with respect to the implementation, training, updating, auditing and enforcement issues arising from the implementation of the Red Flags Rule.
2. The Identity Protection Committee shall meet as necessary to review the administrative functions of the Program.
3. Each member of the Identity Protection Committee will be responsible for ensuring that their respective departmental policies that support and reinforce the Program are maintained and updated to support BHSF's continued commitment to protect and secure patient information. As the need arises, the committee members will update existing policies and implement new policies to support the Program.
4. As the Program Manager, members of the Identity Protection Committee, will ensure that the policies and procedures detailed in the Identity Protection Program are executed.

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")
- Emergency Medical Treatment and Active Labor Act, 42 C.F.R, (EMTALA)
- Fair Credit Reporting Act of 1970, 15 U.S.C. 1681 et. seq., as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 regulations, 16 C.F.R. 681 (Red Flags Rule)
- Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. 160 and 164 (HIPAA)
- Notification requirements of § 817.5681, Fla. Stat. (Florida ID Theft Notification Law)
- Special Publications:
    - Dixon, Pam and Gellman Robert, Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, World Privacy Forum, 9/24/2008.

- ID theft resources at the Federal Trade Commissionhttp://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:

- Corporate HIPAA Privacy Policies
- 10000-74220-703.00 Baptist Health South Florida Identity Protection Program
- Attachment – 10000-74220-703.00A – Exhibit A Red Flags
- Attachment – 10000-74220-703.00B - Exhibit B Related BHSF Policies and Procedures

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.