POLICY TITLE: 703.00 Baptist Health South Florida Identity Protection Program

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.

The Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003 ("**FACTA**") apply to creditors who maintain covered accounts. Hospitals (facilities) are unique in that, unlike financial institutions that voluntarily extend credit and benefit from extending credit, they are in many instances obligated to provide services to individuals under various laws and regulations (e.g., Emergency Medical Treatment and Active

Labor Act ("**EMTALA**") and rules governing tax exempt entities) and extend credit solely as a necessity of collecting payment for the services rendered to individuals in need.

The purpose of the Program is to detect, prevent, and mitigate identity theft in connection with information held in connection with Patient Accounts maintained by BHSF in which it accepts multiple payments for goods or services provided by BHSF when such accounts are primarily for personal, family or household purposes or accounts that contain information that could be used to steal the identity of the individual who is the subject of the information ("covered accounts"). Further, the purpose of the Program is to control reasonably foreseeable risks of identity theft to Patients and to maintain the safety and soundness of BHSF from identity theft. The Program will function in coordination with other efforts of BHSF to secure protected health information in accordance with HIPAA and other applicable federal and state laws. BHSF delegates to the Identity Protection Committee ("Program Manager") the duty of further defining the Program and overseeing the implementation and administration of the Program.

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 Identity Protection Program (the "Program"), developed by BHSF, to assist in the detection, prevention and mitigation of identity theft that may occur with respect to information contained in certain accounts of Patients that are created and maintained by BHSF.

SCOPE/APPLICABILITY:

This policy applies to Baptist Health personnel charged with implementing The Program and BHSF entities and departments that offer or maintain "covered accounts" or use consumer reports obtained from a consumer reporting agency.

PROCEDURES TO ENSURE COMPLIANCE:

1. Administration of the Program
    a. Oversight of Program:
        i. The Baptist Health South Florida Finance and Insurance Board Committee approves the initial Program and thereafter will be involved, through a designated senior management group, in the oversight, development, implementation and administration for the program. Oversight of the Program has been delegated to the Identity Protection Committee (for purposes of this policy this committee will be collectively be referred to as the "Program Manager"), and as such, the responsibilities include:
            1) Implementation of the Program;
            2) Training appropriate BHSF staff on the Program;
            3) Auditing compliance by reviewing reports prepared by staff regarding compliance with the Program and applicable laws and regulations;
            4) Updating and approving material changes in the Program periodically to reflect changing risks to patients or the safety of BHSF from identity theft, and
            5) Periodically reporting to the BHSF Board regarding the success of the Program and incidents of identity theft or attempted identity theft.
2. Reports
    a. In general, the Program Manager and its staff are responsible for the development, implementation, and administration of the Program and should report to the designated Board Committee at least annually, in compliance with the Program and applicable laws and regulations.
    b. Contents of Report
        i. The report should address material matters related to the Program and evaluate issues such as:

1) The effectiveness of the policies and procedures of BHSF in addressing the risk of identity theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
2) Arrangements with third parties that maintain or use Patient information that could be used for identity theft;
3) Significant incidents involving identity theft or attempted identity theft and management's response; and
4) Recommendations for material changes to the Program.

3. Oversight of Service Providers
   a. Whenever BHSF engages a service provider to perform an activity in connection with one or more covered accounts, BHSF shall take reasonable steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. BHSF shall contractually require the service provider to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and to report the Red Flags to BHSF to take appropriate steps to either prevent or mitigate identity theft.
4. Evaluation & Red Flags
   a. Initial Evaluation. The Program Manager shall, upon adoption of the Program, identify and evaluate covered accounts and determine:
      i. The types of covered accounts BHSF offers or maintains;
      ii. The methods BHSF uses to open its covered accounts;
      iii. The methods BHSF uses to access its covered accounts, if any; and
      iv. Any previous experiences BHSF has had with identity theft.
5. Periodic Updates
   a. The Program Manager shall periodically update the Program (including Red Flags) to reflect changes in the risk to patients or to the safety, and soundness, of BHSF from identity theft, based on factors such as:
      i. The experiences of BHSF with identity theft;
      ii. Changes in methods of identity theft;
      iii. Changes in methods to detect, prevent, and mitigate identity theft;
      iv. Changes in the types of accounts that BHSF offers or maintains; and
      v. Changes in the business arrangements of facilities, including mergers, acquisitions, alliances, joint ventures, and arrangements with third parties that have access to information in facility's covered accounts.
6. Identifying Red Flags
   a. Based upon the evaluations referenced above, the Program Manager shall identify system mechanisms and controls to detect and prevent incidents of identity theft using information about patterns, practices or activities that lead to a suspicion of identity theft or an attempt to steal another's identity ("Red Flags"). A current list of Red Flags is attached to this Policy as Exhibit A. The Program Manager shall periodically review and update the Red Flags and is authorized to update Exhibit A to reflect any changes deemed necessary.
7. Verification of Identify of Patient & Detecting Red Flags
   a. BHSF has developed policies and procedures that address activities involving the use of patient information from the time of the registration until the completion of all care and transactions related to the patient's covered account. The purpose of these policies and procedures is to ensure patients are properly identified and to protect the confidentiality of patient information. Such policies and procedures, as identified by the Program Manager, are referenced in this policy, and will be amended as the need arises. The Program Manager shall periodically review the process of verifying patient information, giving consideration to the objective of this policy and other regulatory considerations with respect to the admission and treatment of patients, including but not limited to EMTALA**.**
8. Preventing and Mitigating Identity Theft
   a. BHSF staff who identify Red Flags and are unable to resolve the identity issue should report the issue to their supervisor, manager or lead worker ("BHSF leader"). The BHSF leader will then assess the discrepancy and determine whether the identity issue can be resolved within the Department. If the leader is not able to resolve the identity issue, they should report the occurrence to the Corporate Privacy Office to investigate. The Corporate Privacy Office will determine the appropriate response to the Red Flag detected.

b. The response to the Red Flags will be designed to prevent and mitigate identity theft. This response should be commensurate with the degree of risk posed with the intention of preventing and mitigating identity theft. In determining an appropriate response, aggravating factors that may heighten the risk of identity theft, such as a data security incident or notice that a patient has provided information to someone fraudulently should be considered. Any necessary response should only be performed by the Corporate Privacy Office. Appropriate responses may include, but are not limited to, the following:
   i. Monitoring a covered account for evidence of identity theft;
   ii. Contacting the patient to verify the information or that the services were in fact received;
   iii. Reopening a covered account with a new account number or refusing to open a covered account;
   iv. Not attempting to collect on a covered account;
   v. Notifying law enforcement; or
   vi. Determining that no response is warranted under particular circumstances.

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 Commission http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:

- Corporate HIPAA Privacy Policies
- 10000-74220-702.00 Baptist Health South Florida Identity Protection Committee
- 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.