POLICY TITLE: 203.00 Safeguards – Physical Safeguards to Electronic Protected Health Information (ePHI)

Responsible Department: Corporate Privacy Office

Creation Date: 11/13/2013
Review Date: 2021/12/13
Revision Date: 2021/12/13

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): 2021/12/14

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 covered entity 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. Baptist Health must comply with the applicable standards, implementation specifications, and requirements with respect to electronic protected health information maintained by Baptist Health.

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 safeguarding of patient information. 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 implementation of systems which ensure that the physical access to any Baptist Health electronic information system and the facility or facilities in which they are housed is limited, while ensuring that proper authorized access is allowed.

SCOPE/APPLICABILITY:
This policy applies to Baptist Health, its affiliates, all workforce members, and others as described below.

- **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. Physical Safeguards: physical measures, policies, and procedures to protect a covered entity or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
2. Facility: physical premises and the interior and exterior of a building(s).

PROCEDURES TO ENSURE COMPLIANCE:

1. Baptist Health and its business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
   d. Ensure compliance by its workforce.
2. Facility Access Controls
   a. Baptist Health shall implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that proper authorized access is allowed.
3. Contingency Operations
   a. Baptist Health shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
4. Facility Security Plan
   a. Baptist Health shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
5. Access Control and Validation
   a. Baptist Health shall implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
6. Maintenance Records
   a. Baptist Health shall implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
7. Workstation use
   a. Baptist Health shall implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
8. Workstation security
   a. Baptist Health shall implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
9. Device and Media Controls.

a. Baptist Health shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

10. Disposal
    a. Baptist Health shall implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
11. Media Re-Use
    a. Baptist Health shall implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
12. Accountability
    a. Baptist Health shall maintain a record of the movements of hardware and electronic media and any person responsible thereafter.
13. Data Backup and Storage
    a. Baptist Health shall create a retrievable and identical copy of the electronic protected health information, when needed, before movement of equipment.
14. Security Badges
    a. Badges will be issued:
        i. By the Director of Pastoral Care for Baptist Health members of the clergy;
        ii. By the Supply Chain Services department to vendors; and
        iii. By the Human Resources and Security departments to workforce member, medical staff member, student, independent contractor or other.
    b. The Patient Access departments of each Baptist Health facility shall issue wrist security badges/identifications to all patients admitted for inpatient services.
    c. Badges will be used by:
        i. Baptist Health employees and other workforce members are expected to wear their security badges when on the premises of a Baptist Health facility.
        ii. Any person without a badge shall be presumed to be a patient's visitor. Visitors may be present only in waiting rooms or the room of a patient who has assented to their presence. Assent may be inferred from the circumstances. If there is any doubt or, in the case of shared rooms, ask the patient, if reasonably possible, before disclosing any patient information in the presence of any person without a badge.

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
- Technology & Digital 145 - Permanent Access Badge System
- Technology & Digital 145 – Procedure: Permanent Access Badge System
- Technology & Digital 169 - Visitor Management: Fast Pass System
- Technology & Digital 169 - Procedure Visitor Management System: Fast Pass System
- Human Resources 5275 - Dress Code

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.