



POLICY TITLE: 201.30 Safeguards – Data and Systems Integrity

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: Anthony Longo

Title: Vice President, Chief Information Security 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. This policy governs good system practices for Data and Systems Integrity

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. Baptist Health's policy is to comply with applicable state and federal regarding systems security and access controls.

SCOPE/APPLICABILITY:

This policy applies to the individual entity department directors and the Technology & Digital department when determining and providing job-appropriate levels of access to patient information maintained electronically by members of the BHSF workforce 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.

PROCEDURES TO ENSURE COMPLIANCE:

1. The HIPAA Privacy Rule and various state regulations require Baptist Health to implement reasonable safeguards to protect the privacy of patient information.
 - a. The federal privacy regulation requires the establishment and implementation of technical, physical and administrative safeguards.
 - b. Baptist Health's policy is to comply with applicable state and federal laws regarding the safeguarding of patient information.
 - c. These policies have been established to adequately safeguard patient information and must be followed by all personnel.
 - d. The Technology & Digital department shall implement and continually evaluate systems security to protect patient information maintained electronically from unauthorized and inadvertent access or disclosure by implementing processes and controls to ensure compliance with the HIPAA Security Rule.

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
- 10000-74220-200.00 General Rule Regarding Safeguarding of Patient Health Information
- Technology & Digital 159.00 - Unified Corporate Policy for Compliance with the HIPAA Security Rule
- Human Resources 5225 – Unauthorized release of confidential information

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.