POLICY TITLE: 600.00 Compliance and Implementation – General Rule Regarding Privacy Compliance and Implementation

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. This policy supports implementation of the Administrative Requirements of the HIPAA Privacy Rule. Baptist Health's policy is to comply with applicable state and federal laws regarding in establishing and implementing these administrative requirements.

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 compliance and implementation of the HIPAA Privacy Rule and BHSF's Privacy Program.

SCOPE/APPLICABILITY:
This policy applies to the Corporate Privacy Office, Office of General Counsel, and all workforce members, and others as described below charged with implementing federal privacy regulations under HIPAA. .

- **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:

The HIPAA Privacy Rule requires Baptist Health to adopt policies and implement administrative procedures to ensure compliance with the privacy rule.

1. Privacy Official: Baptist Health must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
2. To this end, the designated privacy official, or Chief Privacy Officer shall ensure that Baptist Health:
    a. Takes the necessary steps to adopt corporate HIPAA policies and procedures, and to make them enforceable with respect to Baptist Health workforce members, including employees, volunteers, licensed health care professionals, and medical staff members, and other individuals who may access, use, and disclose Baptist Health patient information.
    b. Implements privacy policies and procedures, including oversight over revisions to facility policies and any implementation guidance for procedures.
        i. Baptist Health must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements under the HIPAA Privacy Rule.
        ii. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a Baptist Health, to ensure such compliance.
    c. Engages in ongoing evaluation of the need for changes to the corporate privacy policies and procedures and facility policies and/or implementation guides to assure compliance with applicable state and federal laws.
        i. Baptist Health must change its policies and procedures as necessary and appropriate to comply with changes in the law.
            1) Whenever there is a change in law that necessitates a change to the Baptist Health's policies or procedures, the Chief Privacy Officer must promptly document and implement the revised policy or procedure; and
            2) If the change in law materially affects the content of the Notice of Privacy Practices ("NPP" or "the Notice"), the Chief Privacy Officer must promptly make the appropriate revisions to the Notice.
        ii. Baptist Health may make any other changes to its privacy policies and procedures at any time, provided that the changes are documented and implemented in accordance the HIPAA Privacy Rule.
    d. In conjunction with the Human Resources Department, provides job-based training on applicable privacy policies and procedures to individuals covered by this policy.
        i. Baptist Health must train all workforce members, medical staff members, students, independent contractors or others on the policies and procedures with respect to protected health information required by the HIPAA Privacy Rule, as necessary and appropriate for its workforce members, and others covered by this policy to carry out their functions within the covered entity.
    e. Establishes an internal system to respond to privacy complaints by Baptist Health employees, workforce members, and others covered by this policy and members of the public in a non-retaliatory manner.
        i. Establishes a process for patients, their families and members of the general public to ask questions and to submit complaints about Baptist Health privacy practices, or the actions of workforce members, and others covered by this policy

ii. Ensures that the Patient Experience department implements a procedure for documenting privacy complaints in writing, including offering to complete the complaint form for the patient, if specifically requested and appropriate. Whether or not the patient indicates a desire to file a complaint, the Patient Experience department shall prepare and submit an incident report with respect to all aggressive questions that are critical of Baptist Health or its employees' privacy behavior.

iii. Works with Human Resources, Corporate Compliance, General Counsel and other BHSF departments as needed to ensure that no individual covered by this policy intimidates, threatens, coerces, discriminates against, or takes other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by the Privacy Rule, including the filing of a complaint.

iv. The Chief Privacy Officer together with the Human Resources department shall investigate any allegations of intimidating or retaliatory actions and resolve any issues.

v. Investigates privacy complaints involving a Baptist Health facility without intimidation or threat.

f. Mitigates, to the extent practicable, any harmful effect of an improper use or disclosure of protected health information in violation of its policies and procedures or the requirements of the privacy rule by Baptist Health or its business associate.

i. Once the Chief Privacy Officer knows of a use or disclosure in violation of the HIPAA Privacy Policies, the Chief Privacy Officer, in consultation with Corporate Compliance, Risk Management, Human Resources and Office of General Counsel as may be necessary or appropriate, must take prompt action to mitigate any harmful effect of the violation to the extent practicable.

ii. In conjunction with Human Resources, the Chief Privacy Officer shall apply appropriate sanctions against Baptist Health workforce members who violate the HIPAA privacy policies or the Privacy Rule.

g. A Privacy /Security Review Board shall be established which includes individuals from the Privacy Office and Technology & Digital Security.

i. The Privacy /Security Review Board also shall provide ongoing, assistance to the BHSF Chief Privacy Officer with regard to the implementation of the HIPAA policies and procedures and the obligations and duties assigned to the BHSF Chief Privacy Officer.

ii. The Privacy /Security Review Board shall serve in an advisory capacity to the Chief Privacy Officer with respect to any implementation, training, or enforcement issue arising from implementation of the HIPAA Privacy Rule.

iii. The number and composition of the Privacy /Security Review Board shall be established by Baptist Health in consultation with the Chief Privacy Officer and the Chief Information Security Officer to enable the Chief Privacy Officer to have ready access to issues and views of the various Baptist Health and all constituents who are bound by Baptist Health's HIPAA privacy policies and procedures.

iv. The Privacy /Security Review Board shall meet as necessary at the request of the Chief Privacy Officer to discuss any issues related to implementation of the HIPAA policies and procedures.

v. The Privacy / Security Review Board shall report incidents directly to the Cyber Security Council as needed.

3. Documentation of Compliance

a. Baptist Health must maintain/retain the privacy policies and procedures in written or electronic form.

b. If a communication is required by the privacy rule to be in writing, the Corporate Privacy Office must maintain such writing, or an electronic copy, as documentation.

c. If an action, activity, or designation is required by the Privacy Rule to be documented, the Corporate Privacy Office maintains a written or electronic record of such action, activity, or designation.

d. Baptist Health must maintain documentation sufficient to meet its burden of proof in the event of a use or disclosure in violation of the Privacy Rule.

i. Baptist Health or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by the Privacy Rule, Notification In The Case of a Breach of Unsecured Protected Health Information*;* or that the use or disclosure did not constitute a breach, as defined by the Privacy Rule.

ii. Baptist Health must retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

e. Responds appropriately to investigations or compliance reviews by the Secretary of the Department of Health and Human Services.

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
- 10000-74220-602.10 Compliance and Implementation – Privacy Training of BHSF Workforce
- 10000-74220-605.20 Compliance and Implementation – Sanctions for Privacy Violations
- 10000-74220-701.00 Privacy and Security Incident Reporting and Response
- 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.