POLICY TITLE: 001.00 Unified Corporate Privacy Policy on HIPAA Compliance

Responsible Department: Corporate Privacy Office

Creation Date: 04/07/2003
Review Date: 2021/12/15
Revision Date: 2021/12/15

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 sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

In compliance with state and federal laws, Baptist Health South Florida ("BHSF" or "Baptist Health") has established a Unified Corporate Policy on HIPAA Compliance to govern our business practices and provide guidance to our workforce in order to protect the confidentiality of patient health information and establish certain individual privacy rights.

POLICY:

It is the policy of BHSF 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. Detailed policies ("HIPAA Privacy Policies") shall ensure that anyone covered by this policy shall have precise instructions for implementing this policy in patient care, administrative and public settings.

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.
Baptist Health affiliates are directly affected by the federal privacy regulation promulgated under the Health Insurance Portability and Accountability Act ("HIPAA") of 1996.

The BHSF affiliates can be found on the BHSF website at: HIPAA Notice of Privacy Practices (baptisthealth.net). These affiliates are referred to in this policy as "BHSF facilities" or "Baptist Health facilities." This policy provides a single, integrated strategy for the BHSF facilities and their medical staffs to meet the HIPAA requirements as "Baptist Health," the single affiliated covered entity designated in this policy below, exclusively for purposes of HIPAA compliance.

PROCEDURES TO ENSURE COMPLIANCE:
The Chief Privacy Officer shall coordinate with the appropriate stakeholders to ensure that all workforce members and others who are subject to this policy have access to the HIPAA Privacy Policies for reference in connection with the performance of their job or activity at any BHSF facility.

1. Corporate Policy Regarding Individual Rights Granted by HIPAA:
    a. Notice and Choice. All BHSF facilities shall use the Baptist Health Notice of Privacy Practices.
        i. The "Notice" shall comply with applicable law, accommodate any changes in corporate policy and set forth an effective date.
            1) The Notice shall be freely available to the public upon request. The Notice shall be available in all BHSF facility Admitting/Registration and/or Patient Experience departments, posted on corporate websites and copies shall be furnished to each patient at the first service delivery.
            2) Any proposed revision to the Notice shall not be effective unless it is reviewed and approved by the BHSF Chief Privacy Officer and the BHSF Office of General Counsel.
        ii. BHSF facilities must make a good faith effort to obtain the patient's acknowledgment of receipt of the Notice and the patient's consent to use and disclose health information from all patients using the revised face sheet or to document their efforts and failure to do so.
            1) The acknowledgement of receipt of the Notice and the consent to use and/or disclose health information must comply with applicable federal and state laws.
            2) Any proposed revision to the acknowledgment and consent section of the face sheet shall not be effective unless it is reviewed and approved by the BHSF Chief Privacy Officer and the BHSF Office of General Counsel.
    b. Rights to Request Enhanced Privacy.
        i. Restrictions on Use. HIPAA regulations establish a patient's right to request restrictions on the use and/or disclosure of protected health information, including restrictions on use of information in treatment, and for payment and administrative purposes. This right shall be carefully implemented so as not to undermine BHSF facilities' ability to efficiently and effectively deliver care and manage their activities.
            1) Baptist Health is not required to accept such requests and will reject any patient request which seeks to limit access by a health care professional to the patient's protected health information for treatment purposes, or which precludes our ability to be paid for services rendered.

2) Patients have a right to request that a healthcare provider comply with the patient's request for restriction of disclosure to a health plan for purposes of payment or healthcare operations when the patient health information pertains to a service for which the healthcare provider has been paid in full by the patient "out of pocket."
3) This right may be exercised only by submission of a written request as provided in the HIPAA Privacy Policies.
4) Any such request may be approved in the sole discretion of the BHSF Chief Privacy Officer by issuance of a written notice of acceptance.
5) No medical staff member, licensed health care professional, employee, corporate officer, contractor, clergyman, or volunteer has authority to approve patient requests for restrictions on use of information entered into the records of Baptist Health or a BHSF facility.

ii. Alternative Communications. Baptist Health will accommodate reasonable requests for BHSF facility communications to be sent to an alternative address or phone number. This accommodation will not apply to mammography screening related correspondence or results.
1) This right may be exercised only by submission of a written request as provided in the HIPAA Privacy Policies.
2) The BHSF Chief Privacy Officer and/or Admitting/Registration Department are authorized to determine the reasonableness of such requests and to approve them by issuance of a written notice of acceptance.
3) No medical staff member, licensed health care professional, employee, corporate officer, contractor, clergyman, or volunteer has authority to approve patient requests for confidential communication of matters that concern treatment, payment, or administrative activities of Baptist Health or a BHSF facility.

iii. Presence in Facility. Each BHSF hospital facility will maintain a directory to permit friends, family members, and other interested persons who ask for the patient by name to locate hospitalized individuals. At the patient's request, Baptist Health will accommodate a reasonable request not to be listed in the facility directory.

c. Patients' Rights To Access and Inspect Certain Information.
i. All BHSF facilities shall comply with applicable state and federal law in providing patients with access to medical, billing and other information about them that is maintained in designated record sets using the protocols established in the HIPAA Privacy Policies.

d. Patients' Rights to Amend Certain Information.
i. All BHSF facilities shall comply with applicable state and federal law that allows patients to request for an amendment of incorrect or incomplete health information in a designated record set or correct errors in medical and billing records.
ii. The HIPAA Privacy Policies provides a protocol for receiving such corrections and making annotations or addendums.

e. Patients' Rights to an Accounting of Disclosures.
i. All BHSF facilities shall comply with applicable federal law that permits patients to obtain an accounting of certain disclosures of information for purposes other than treatment, payment or administrative activities.
ii. A process for creating the records to provide such an accounting and for responding to patient requests is provided in the HIPAA Privacy Policies.

f. Patients' Rights to File a Complaint.
i. All BHSF facilities shall follow-up on patient complaints as provided in the HIPAA Privacy Policies.

2. Corporate Policy Regarding Safeguards for Protecting Patient Information Created or received by or on behalf of Baptist Health:
a. Minimum Necessary. Every medical staff member, employee, volunteer, licensed health care professional or contractor who uses, discloses, or requests patient information on behalf of Baptist Health shall make reasonable efforts to limit protected health information to the minimum necessary to accomplish the authorized purpose of the use, disclosure or request, including minimizing incidental disclosures. The procedures for implementing this policy vary based on the intended purpose of the use, disclosure or request, as provided in the HIPAA Privacy Policies.

b. Administrative Safeguards:
   i. BHSF Facility Workforce. BHSF facilities shall implement policies to hold employees, volunteers, licensed health care professionals, medical staff members and contractors accountable for ensuring that they do not use or disclose protected health information except for patient care functions of the facility in which the patient received care, or as provided in the HIPAA Privacy Policies.
   ii. Business Associates. A third party contractor of any Baptist Health facility may not receive, create, maintain or transmit protected health information in order to provide a service or perform a function for or on behalf of Baptist Health unless the third party has signed a Business Associate Agreement.
   iii. De-Identification; Data Use Agreements. When a third party performs administrative analysis, Baptist Health facilities shall use a Data Use Agreement or shall try to obtain approval from the Baptist Health Corporate Privacy Office before transmitting data.

c. Technical Safeguards.
   i. Baptist Health shall issue information systems IDs and credentials that permit the assignment of job-appropriate levels of access to electronically maintained patient information. Baptist Health shall ensure that credentials and IDs are revoked when employment, contract, licensed health care professionals access to electronic information, or medical staff privileges are terminated.
   ii. Baptist Health shall implement and continually evaluate systems security to protect public confidence that information is secure from unauthorized and inadvertent access or disclosure, and to protect Baptist Health confidence in the integrity of the information as a basis for patient care and business operations.

d. Physical Safeguards.
   i. Access to rooms and locations where patient information is maintained shall be secured.
   ii. Paper charts of recently discharged patients shall be removed from patient care areas and promptly routed to the appropriate Health Information Management Department for records retention purposes.
   iii. BHSF facilities shall issue identification badges and require that they be worn by employees, volunteers and other workforce members.

3. Standards for Using and Disclosing Patient Information:
   a. Treatment. Ethical and professional standards assuring the provision of quality health care and the immediate demands of attending to the physical, social and psychological needs of a patient who is seeking treatment from Baptist Health facilities are the primary considerations in deciding how to use or disclose patient information.
      i. Subject to this primary consideration, every employee, licensed health care professional, medical staff member or volunteer must make reasonable efforts to limit the patient information to the minimum necessary to accomplish the intended purpose.
      ii. It is never reasonable to limit information when doing so might influence an action or decision by any caregiver that could adversely affect the patient's health care or well being.
   b. Payment. Provided that consent has been obtained upon admission, patient information may be used and disclosed to obtain payment for services rendered by Baptist Health facilities and to assist another provider in obtaining payment for related services, unless Baptist Health has agreed, in writing, to a restriction on use or disclosure of the information as provided in this policy and the HIPAA Privacy Policies.
   c. Administrative Activities. Patient information may be used for Baptist Health facilities' administrative analyses and activities, so long as arrangements are made for using the minimum necessary information for the purpose, and appropriate safeguards are implemented. Any use of patient information, including demographic information, for fundraising or for marketing shall meet the requirements of the HIPAA Privacy Policies.
   d. Research. No Baptist Health facilities' patient information shall be used or disclosed for research, whether by employees, affiliated medical staff members or third parties, unless the researcher meets the requirements of one of the options provided in the HIPAA Privacy Policies.
   e. Use of Patient Information by Third Parties. Patient information may be disclosed to third parties for treatment purposes, payment purposes or for health care operations disclosures required by law. Otherwise, patient authorization is required before the third party disclosure is made.

4. Corporate Policy Regarding Organizational Structure and Accountability for HIPAA Compliance:
   a. BHSF is committed to establishing a compliance structure for itself and its affiliates to meet the requirements of the HIPAA privacy regulation and state privacy laws in a manner that ensures the necessary flow of health information for efficient, quality patient care and facility operations, as provided in this policy.
   b. Hybrid Entities. Each BHSF affiliate that performs both covered functions and non-covered functions is designated a hybrid entity for purposes of HIPAA compliance. Covered functions are treatment and payment activities.
   c. The BHSF affiliates that perform covered functions are identified on the Baptist Health South Florida website at HIPAA Notice of Privacy Practices (baptisthealth.net) collectively, "BHSF facilities" or "Baptist Health facilities".
   d. BHSF employees are included in the health care component of each BHSF facility and are considered part of the workforce of each BHSF facility to the extent they perform covered functions for the facility and/or perform business associate-type functions, including legal, auditing, administrative, management or billing services, for or on behalf of the BHSF facility.
   e. Each BHSF facility participating must designate its health care component, which must include all of its divisions, departments, or components that perform covered functions and that create or receive protected health information in order to perform a function or provide a service related to the BHSF facility's covered functions.
   f. Research activities shall be excluded from the BHSF facility's health care component as provided in the HIPAA Privacy Policies.
   g. Each BHSF facility shall submit a description identifying any of its components or activities that are excluded from its health care component(s) and any subsequent changes thereto, to the BHSF Chief Privacy Officer.
      i. Components or activities that are excluded from a facility's health care component (such as research) are governed by this HIPAA policy only with respect to how they obtain patient information from a health care component. Other information obtained or maintained by an excluded component shall be governed by other applicable laws and facility policies.
      ii. A BHSF facility may share protected health information from its health care component(s) with excluded components only if the disclosure is permitted under the HIPAA Privacy Policies governing use and disclosure of patient information to a third party.
      iii. Each BHSF facility must implement reasonable and appropriate safeguards to ensure that protected health information is not improperly shared outside the entity's health care component.
      iv. All workforce members and individuals covered by this policy that have responsibilities both within a BHSF facility's health care component and outside it, shall not use protected health information for non-health care component purposes, unless disclosure of the information to the non-health care component is otherwise permissible if the disclosure were made to a separate entity.
   h. Single Affiliated Covered Entity and Business Associates. The health care component(s) of each BHSF facility, including the workforce of each BHSF facility, shall be designated the Baptist Health Affiliated Single Covered Entity, also called Baptist Health, for purposes of HIPAA compliance.
      i. The BHSF facilities participating in Baptist Health may share protected health information between and among their health care components for joint health care operations purposes and for other activities permissible under this policy and the HIPAA Privacy Policies implementing procedures.
      ii. By law, BHSF affiliates that do not provide treatment are not included in the Baptist Health Affiliated Single Covered Entity. Where the BHSF affiliate provides business associate-type services, including billing and collection services, insurance, financing or other services that require access to patient information for any of the Baptist Health entities, the affiliate is a business associate of Baptist Health.
      iii. Where arrangements for services by a contractor involve access to or creation of patient information on behalf of any of the BHSF facilities, the responsible BHSF facility executive is authorized to enter into the required business associate agreement that will be made a part of, or incorporated into, the underlying agreement with the third party.

1) The responsible executive, in conjunction with the BHSF Supply Chain Services department, shall oversee the business associate agreements, including negotiation and enforcement, for services involving use or disclosure of patient information that may be required by any or all of the BHSF facilities participating in Baptist Health.
2) The responsible executive, in conjunction with the BHSF Supply Chain Services Department shall be responsible for establishing a process to obtain relevant information from business associates when patients' rights are exercised under HIPAA and for confirming that, upon termination or expiration of the business associate agreement, all protected health information is returned or destroyed consistent with the provisions in the business associate agreement.
3) Each BHSF facility shall have its business associate agreements within the BHSF family signed and administered in accordance with this policy.
4) BHSF may enter into business associate agreements on behalf of the BHSF facilities, as needed.

i. Organized Health Care Arrangements with Medical Staff Members. Each BHSF facility may be designated part of a separate organized health care arrangement ("OHCA") with the medical staff members that have privileges at such facility.
   i. Each BHSF facility shall have all of its medical staff members rendering care at the BHSF facility sign the OHCA participation agreement.
   ii. No medical staff member or allied health professional has authority to act on behalf of Baptist Health or any BHSF facility with regard to a request by any patient or the patient's personal representative to exercise the patient's rights under HIPAA, except as provided in the HIPAA Privacy Policies regarding patient rights.
   iii. OHCA participants may share or disclose protected health information only for:
      1) Treatment and payment activities,
      2) The joint health care operations of the OHCA, and
      3) As provided under the HIPAA Privacy Policies.
   iv. Physicians who are not credentialed as BHSF medical staff members with electronic access to diagnostic test results may share or disclose protected health information only:
      1) For treatment and payment activities,
      2) As provided in the signed Net Access agreement, and
      3) As provided under the HIPAA Privacy Policies.

j. Health Plans.
   i. BHSF sponsors health plans that are separate covered entities under HIPAA ("Health Plans") and BHSF employees provide certain administration functions on behalf of these health plans. These Health Plans and the administration functions provided on their behalf are not part of the health care component and are not subject to the other implementing policies set forth in Sections 4c, 4d, 4e and 4g of this policy. These Health Plans and the administrative functions provided by BHSF on their behalf are subject to separate policies and procedures set forth in the HIPAA Privacy Group Health Plan Policy Manual.

5. Corporate Policy Regarding Implementation and Oversight Compliance:
   a. Administration. A single administrative structure is established for implementation of this policy, as follows.
      i. The BHSF Chief Privacy Officer is charged with supporting the HIPAA implementation efforts of all BHSF facilities participating in the Baptist Health Single Affiliated Covered Entity, including:
         1) Implementation of the BHSF HIPAA Privacy policies and procedures, and reviewing and recommending any proposed changes to the policies or the procedures manual;
         2) Receiving complaints from BHSF employees, volunteers, licensed health care professionals or medical staff members and patients regarding a violation or suspected violation of such policies and procedures;
         3) Developing and overseeing employee training and compliance;
         4) Supporting the activities of departments and divisions that are most directly affected by the new requirements.
      ii. A Privacy / Security Review Board shall be established which includes individuals from the Corporate Privacy Office and IT Systems Security. The Privacy /Security Review Board shall meet as necessary to

discuss any issues related to implementation of the HIPAA policies and procedures. 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. The Privacy / Security Review Board shall report incidents directly to the Chairman of the Cyber Security Council as needed.

iii. Each BHSF facility shall designate the Patient Experience or Risk Management department as the facility liaison for purposes of HIPAA compliance. These liaisons will coordinate with the BHSF Chief Privacy Officer with respect to HIPAA activities in the BHSF facility.
   1) All questions from patients or the general public regarding BHSF HIPAA policies and procedures, and requests to exercise rights granted by HIPAA, shall be coordinated by the facility liaison with the support and assistance of the BHSF Chief Privacy Officer.
   2) Each facility liaison must promptly report any patient or workforce complaints of a violation or suspected violation of BHSF HIPAA policies and procedures to the BHSF Chief Privacy Officer.

iv. Each BHSF facility shall designate two or more health care professionals to participate in reviewing any written patient appeals regarding BHSF's denial of access to their medical records.

v. HIPAA Privacy Policies are hereby adopted for implementation of these policies at the BHSF facility level.
   1) Each BHSF facility shall implement these policies and procedures, including training its personnel on the HIPAA Privacy Policies.
   2) Each BHSF facility shall modify its existing policies and procedures where necessary and appropriate to comply with these policies and implement the HIPAA Privacy Policies.
   3) Questions regarding and/or proposed modifications of the HIPAA Privacy Policies or these policies must be addressed to the BHSF Chief Privacy Officer. All proposed modifications, including any deviations from the HIPAA Privacy Policies for a specific BHSF facility must be proposed to and approved by the BHSF Chief Privacy Officer prior to implementation.

6. Complaints and Mitigation.
   a. The BHSF Chief Privacy Officer shall administer the process for receiving public and employee complaints or suspicions of a violation of BHSF's HIPAA policies and procedures, whether directly from patients or family members, or through BHSF facility liaisons, including procedures for:
      i. Investigating complaints;
      ii. Appropriate mitigation and remedial actions, including recommendations of sanctions for employees or contractors; and
      iii. Ensuring that whistleblowers and complainants are not subject to retaliatory action.
   b. Documentation. The BHSF Chief Privacy Officer, in conjunction with the records custodian(s) for each BHSF facility designated record set custodian, shall be responsible for ensuring that archives include copies (written or electronic) of all documents required to be maintained by law for at least six years after the date they were created, or (if later) the date they were last relied upon.
      i. Corporate Documents. Current and superseded copies of the Corporate Policies for HIPAA Implementation, the HIPAA Privacy Policies, and the Notice of Privacy Practices shall be maintained for six years after the date they were last in effect.
      ii. Patient Correspondence. Copies of patient acknowledgements and authorizations shall be maintained as part of the patient's medical record for as long as the medical record is maintained. All correspondence relating to the exercise of patient rights and/or patient complaints shall be maintained for at least six years after receipt.
      iii. Workforce and OHCA Member Documents. OHCA agreements, employee confidentiality agreements, and vendor confidentiality agreements shall be maintained for six years after the date they are terminated. Records of HIPAA training completion shall be maintained for at least six years after termination of the employee or OHCA relationship.
      iv. Net Access agreements signed by non-credentialed BHSF physicians shall be maintained for six years after the date they are terminated.
      v. Research Documents. Documentation authorizing use or disclosure of patient records for research shall be maintained for six years after the date they were last relied upon in disclosing or using information for the research project.

vi. Privacy Office Documentation. The BHSF Chief Privacy Officer shall ensure that a log of the education and HIPAA awareness activities provided in each facility, or in BHSF media, is maintained for at least six years from the date of such training or awareness.

c. Workforce Training and Oversight. The BHSF Chief Privacy Officer shall develop a program for training existing employees, including ongoing training to help each person develop a fuller awareness of and sensitivity to patient privacy issues and ways in which BHSF HIPAA policies and procedures can be enhanced.
   i. Together with Human Resources, the BHSF Chief Privacy Officer shall develop job-appropriate training for new employees, volunteers, licensed health care professionals and medical staff members in the critical aspects of BHSF HIPAA privacy polices and procedures.
   ii. Together with the Human Resources Department, the Chief Privacy Officer shall develop procedures for recommending sanctions for BHSF workforce members, medical staff members, students and independent contractors and others who violate the BHSF HIPAA Privacy Policies.

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
- Information Technology Policy 159 – Unified Corporate Policy for Compliance with the HIPAA Security Rule

ENFORCEMENT & SANCTIONS:

1. Reference: Corporate HIPAA Privacy Policy BHSF-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.