



**POLICY TITLE:** 605.20 Compliance and Implementation – Sanctions for Privacy Violations

**Responsible Department:** Corporate Privacy Office

**Creation Date:** 04/07/2003

**Review Date:** 2021/12/09

**Revision Date:** 2021/12/09

**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):** 2021/12/13

---

## **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. BHSF is committed to protecting proprietary & confidential patient, financial, employee and any other type of protected information. As part of that commitment, the Privacy Office was established to develop and maintain the internal programs to ensure that this information is appropriately used and disclosed for its intended purpose.

## **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.

Baptist Health takes a very strong position in responding to and remediating privacy violations. Any workforce member who inappropriately accesses, uses or discloses Baptist Health's Protected Health Information (PHI) will be subject to corrective action including immediate termination of employment and/or removal of access to Baptist Health's electronic systems. This policy supports the process associated with investigating a privacy incident, in conjunction with Human Resources, when a member of BHSF's workforce is involved. Its objective is to assure consistency in investigating members of BHSF's workforce and in the imposition of sanctions as a result of privacy infractions.

## **SCOPE/APPLICABILITY:**

This procedure applies to the Chief Privacy Officer, the Human Resources department and 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.

Any employee involved in a privacy incident which results in a violation of BHSF policy shall be subject to the appropriate BHSF corrective action.

#### **PROCEDURES TO ENSURE COMPLIANCE:**

Baptist Health must have and apply appropriate sanctions against all workforce members and individuals covered by this policy who fail to comply with its privacy policies and procedures or the requirements set forth by the HIPAA Privacy Rule.

1. **Employees:** The Human Resources department of each BHSF facility, in consultation with the Chief Privacy Officer, shall establish sanctions to be applied against Baptist Health employees, volunteers, and workforce members who fail to comply with the HIPAA Privacy Policies or the Privacy Rule. Such sanctions shall be appropriate to the severity of the infraction and may take into account repeat offenses and willful violation, in accordance with Human Resources 5300 Corrective Action Policy.
2. **Medical Staff:** Sanctions to be applied to members of the medical staff and licensed health care professionals who are members of an Organized Health Care Arrangement ("OHCA") agreement with Baptist Health, shall be determined in accordance with the terms of that agreement. Such sanctions shall be appropriate to the severity of the infraction and may take into account repeat offenses and willful violation, and may include:
  - a. Loss of electronic access to BHSF patient information; or
  - b. Loss of medical staff privileges.
3. **Other:** Sanctions will also be applied to non-BHSF employees, non-affiliated medical staff members, vendors, consultants, students or other non-employed workforce members who have been granted access to BHSF patient information and do not comply with the BHSF HIPAA privacy policies. Such sanctions shall be appropriate to the severity of the infraction and may take into account repeat offenses and willful violation, and may include:
  - a. Limiting or removing electronic access to BHSF patient information.
  - b. Termination from student affiliation, rotation, or other education program.
4. The Chief Privacy Officer shall contact Baptist Health administration, Academic Affairs Leadership, Medical Staff Leadership and/or the Human Resources department when any workforce member or individuals covered by this policy fails to comply with the HIPAA Privacy Policies or the Privacy Rule.
5. The Chief Privacy Officer, in consultation with the Human Resources department and Baptist Health leader, shall determine and apply appropriate employee sanctions for failure to comply with the HIPAA Privacy Policies or the Privacy Rule, except as set forth in the exceptions portion of this policy.
  - a. Human Resources and the Corporate Privacy Office will collaborate during the interview and document all meetings and discussions regarding the interview process and its content.
  - b. The Corporate Privacy Office will recommend actions to be taken for employee remediation if necessary in order to maintain consistency throughout BHSF.

All references to Policies must go to the BHSF Master Copy on the BHSF Intranet; do not rely on other versions / copies of the Policy.

- c. The Human Resources department of each BHSF facility, in consultation with the Chief Privacy Officer and the department leader, shall make a recommendation on the appropriate corrective action if deemed necessary for Baptist Health employees with a privacy violation.
  - d. Any employee involved in a privacy incident which results in a violation of a Privacy Policy shall be subject to the appropriate BHSF corrective action.
    - i. It is understood that each situation is unique and all facts surrounding the violation must be considered, along with the employee's work history, current/recent corrective actions and their role within the organization.
    - ii. The guidelines set below are a general course of action thought out with the specific intent to provide leadership direction for remedial action.
    - iii. Generally, the guidelines should be followed for consistency within BHSF; however, discretion is allowed with the approval of the Human Resources Director in consultation with the Chief Privacy Officer and appropriate BHSF leadership as needed.
    - iv. Deviations: Privacy Sanctions Advisory Board
      - 1) Deviations from recommended corrective action must be reviewed by the Privacy Sanctions Advisory Board
      - 2) Human Resources Director of impacted entity must be included in every deviation review/request.
    - v. Grievances: In accordance with HR 5200, Resolution of Grievances, privacy related corrective actions are not eligible to go through the grievance process.
    - vi. Note that in situations in which it appears that an employee has acted with reckless disregard for the privacy of one or more patients' information, BHSF reserves the right to terminate the employee's employment.
6. Exceptions
- a. No sanction may be applied against any workforce members or individuals covered by this policy
  - b. who:
    - i. Files a complaint with the Secretary of Health and Human Services (HHS) for alleged violations of the Privacy Rule or is involved in other investigations or actions regarding privacy;
    - ii. Opposes any act or practice unlawful under the Privacy Rule, provided that the workforce member, medical staff member, student, independent contractor or other has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve a disclosure of patient information in violation of the Privacy Rule;
    - iii. Believes in good faith that a BHSF facility has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by a facility potentially endangers one or more patients, workers, or the public, and the disclosure of patient information is to:
      - 1) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of a BHSF facility; or
      - 2) An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professionals standards or misconduct by a BHSF facility; or
      - 3) An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the workforce member with regard to the corrective action described in procedure 5C above; or
      - 4) Is the victim of a criminal act discloses patient information to a law enforcement official, the patient information disclosed is about the suspected perpetrator of the criminal act; and the patient information disclosed is limited to the following:
        - a) name and address;
        - b) date and place of birth;
        - c) social security number;
        - d) ABO blood type and rh factor;
        - e) type of injury;
        - f) date and time of treatment;
        - g) date and time of death, if applicable; and

- h) description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
7. The Corporate Privacy Office and the Human Resources department of the applicable BHSF facility shall document any sanctions that are applied in the personnel medical staff or applicable files of the Baptist Health workforce member or individual covered by this policy and retain this documentation as discussed in the applicable HIPAA Privacy Policy.
  - a. In the event that the investigation results in any level of corrective action, a copy of the final corrective action document must be forwarded to the Corporate Privacy Office.

**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
- Information Technology 109 - Computer Identification, Access and Authorization
- Human Resources 5225 - Unauthorized Release of Confidential Information
- Human Resources Attachment - Confidentiality and Non-Disclosure Agreement
- Human Resources 5200 - Resolution of Grievances
- Human Resources 5250 - Employee Conduct
- Human Resources 5300 - Corrective Action
- Human Resources 5270 - Office Gossip
- Human Resources Attachment - Action Plan-Workplace Gossip
- Human Resources 6400 - Mobile Devices at the Workplace
- Human Resources 6750 - Social Media Policy
- Baptist Health's Code of Ethics
- Baptist Health Service Excellence Standards - Privacy and Confidentiality

**ENFORCEMENT & SANCTIONS:**

1. Reference: Corporate Human Resources Policies
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.