POLICY TITLE: 202.00 Safeguards – Safeguards for Verbal, Written, and Electronic Protected Health Information

Responsible Department: Corporate Privacy Office

Creation Date: 2003/04/07
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): 2021/12/20

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.

The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards, and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is a secondary use or disclosure that cannot reasonable be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule. Baptist Health, as a covered entity, has in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures.

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 good safeguards for verbal, written, and electronic Protected Health Information.

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.

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. The federal privacy regulation requires the establishment and implementation of administrative, physical and technical safeguards.
2. This policy has been established to ensure adequate safeguards for patient information and must be followed by all personnel.
3. To illustrate, below are some, but not all, examples of Safeguards for Verbal, Written, and Electronic PHI:
    a. Safeguarding Verbal PHI
        i. Verbal PHI should be protected from inappropriate disclosure.
        ii. All BHSF personnel must ensure that appropriate safeguards are taken when oral communication to third parties, patients, family members, other BHSF personnel and in open-access areas occurs.
        iii. Individuals should avoid discussing patient information in open areas whenever possible, remain attentive to time, place and tone and listen to cues from patients and families.
        iv. Individuals should try to take relatively simple steps, such as speaking quietly when discussing a patient's condition in public areas, avoiding the use of names or other identifying information in conversations and whenever possible, and provide "quiet areas" for protected information exchange.
        v. Note also that oral communications, like any other, are subject to the rule that use and disclosure should be the minimum necessary given roles and responsibilities. (The minimum necessary standard does not apply to exchanges among providers for treatment purposes, whether oral or in any other form.)
    b. Safeguarding Written PHI
        i. Each patient chart shall be safeguarded from unauthorized viewing by using reasonable safeguards, such as utilizing a blank cover page on the front of a clipboard to prevent any information about the patient from being viewed by unauthorized individuals.
        ii. Never leave patient charts in areas where they can be viewed by visitors.
        iii. Always dispose of paper documents and labels in the designated bins.
        iv. Documents containing PHI may not be removed from the department unless you have received prior approval from your leader.
        v. Before handing any patient information to a patient, and/or their family, carefully review the documents to ensure you are providing the right information to the right person.
        vi. Keep paper patient information in a secure location out of view of the public.
        vii. Ensure all non BHSF employees working on your unit are properly identified by the facility and have the proper identification prior to reviewing records; know who is in your area and the reason.

viii. The unit secretary of each nursing floor shall ensure that charts are maintained at the nursing unit when not in use. Visitors and other persons without appropriate credentials shall be kept away from the area where charts are located.

ix. Any employees, workforce members or those with staff privileges who are permitted to use patient information must:
   1) Return any patient charts to the nursing unit after use; and
   2) To the extent that patient charts or clipboards are in use at the bedside, return the chart or clipboard so that it faces the door or wall, if possible.

x. Charts of recently discharged patients shall be removed from patient care areas in order to be processed as soon as it is appropriate.

xi. Employees, workforce members or those with staff privileges who maintain patient information in non-patient care areas should ensure that, if appropriate, locks are installed on the doors of any room and these doors are locked or secured when not present to prevent unauthorized entry and undetected removal of information.

xii. Facsimile Transmission of Patient Information:
   1) Each Baptist Health facility shall attempt to situate all facsimile machines in locations that are not readily accessible to public traffic to prevent unauthorized access to patient information.
   2) Incoming faxes should be promptly routed to their appropriate destination in order to prevent inadvertent disclosures to persons not involved in treatment of the patient.
   3) Prior to sending a facsimile that contains patient information, any person covered by this procedure should confirm that the facsimile number to be used is, in fact, the correct one for the recipient; and
   4) Outgoing manual faxes should contain a cover sheet.

xiii. Printing of Patient Information from a remote location
   1) Employees, workforce members or those with staff privileges who print patient information in remote locations, shall use appropriate safeguards to protect printed documents from the public.
   2) Prior to printing remotely, any person covered by this procedure must carefully select the destination printer to ensure that the printed document is retrieved immediately and safeguarded.
   3) Any person covered by this procedure should destroy all remotely printed documents in an appropriate shredder bin.
   4) Safeguard all printed documents by placing in the secured patient file if applicable.

c. Safeguarding Electronic PHI
   i. Computer screens should be tilted or moved so that information is not visible to the public.
   ii. Users should log-off any computers after accessing patient information before leaving a terminal in an open area which is unattended, even for a few minutes.
   iii. Passwords should ALWAYS be protected and NEVER shared, it may help if you safeguard your passwords the same way as you safeguard your personal ATM PIN, or banking information.
   iv. All email communications containing any patient, financial or BHSF confidential information should be maintained within the Baptist Health/Bethesda email system unless you have received prior authorization/approval from your supervisor AND the information has been encrypted.
   v. Protected Health Information may not be stored on any electronic mobile devices; such as laptops, USB (Thumb Drives), external hard drives, cell phones, tablets (iPads), or cloud storage.
   vi. PHI may never be share, use, or disclose in a Text Message using a personal phone.
   vii. No personal electronic mobile devices should be used in patient care areas (BHSF HR Policy 6400).

4. Questions regarding appropriate safeguards should be directed 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
- Technology & Digital 101.00 – Corporate Systems Security
- Technology & Digital 106.00 - Removal of Systems Access from Terminated & Suspended Employees
- Technology & Digital 109.00 - Computer ID/Log In Access and Authorization
- Technology & Digital 139.00 - Data Encryption for Sensitive or Regulated (Federal, State, etc.) Data while at Rest or in Transit
- 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.