POLICY TITLE: 200.00 General Rule Regarding Safeguarding of Patient 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 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 technical, physical and administrative safeguards.

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 safeguarding of patient 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:

It is Baptist Health's policy to comply with applicable state and federal laws regarding the safeguarding of patient information. These procedures have been established to adequately safeguard patient information and must be followed by all personnel.

To illustrate, below are some, but not all, of the Safeguards set forth by this policy:

1. Administrative Safeguards
    a. Lower the tone of your voice when discussing a patient's condition in an open area.
    b. Avoid discussing patient information in open areas whenever possible.
    c. Listen to your patients and families.
    d. Remain attentive to time, place and tone.
    e. Contact Patient and Guest Services or the Privacy Office in the event a patient or employee wishes to exercise one of their privacy rights. .
    f. Verify in the patient's record, with registration/admitting or with the hospital operator to determine if a patient has opted out of the facility directory prior to releasing any information. Provide the minimum amount of PHI necessary in non treatment situations.
    g. Use best professional judgment to ensure that the person requesting PHI is treating the patient.
    h. When receiving a request for information via telephone, verify the requestor is either the patient or someone involved in their care or treatment or responsible for payment.
        i. If the request is from a family member or friend who would like information about a patient's condition, and the patient is awake, alert, and oriented, pass the call through to the patient (provided they have not opted out of the facility directory).
        ii. If the call comes to the nursing unit, the nurse may ask questions to determine if the caller is involved in the care of the patient which would allow information to be provided.
        iii. If the request is regarding care or treatment of the patient, ask if the person is the treating physician. You may ask a treating physician to fax a note on their letterhead if necessary.
        iv. If the patient is incapacitated, and there is a health care proxy/surrogate involved in the care or treatment of the patient, you may direct the caller to talk to the health care proxy or designated surrogate.
        v. If the request is made to Patient Financial Services and is regarding account information, ask for identifiers such as who the caller is, account number, date of service, date of birth, address, phone number on record, etc.
    i. Remember, if a patient is incapacitated or in emergent situation, please use your best professional judgment when determining whether to notify family and friends of the patient's location or condition. Ask yourself, would the notification be in the best interest of the patient?
2. Physical Safeguards
    a. Safeguard the integrity of the paper record.
    b. Never leave patient charts in areas where they can be viewed by visitors.
    c. Always dispose of paper documents and labels in the designated bins.
    d. Documents containing PHI may not be removed from your department unless you have received prior approval from your leader.

e. 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.
f. Baptist Health South Florida employees must always wear their ID badge when on the premises of a Baptist Health facility.
g. Communicate the concern for privacy to patients and family members in a positive manner such as "to ensure your privacy", or "in order to protect our patient's privacy".
h. Tilt or move your computer screens so that information is not visible to the public.
i. Keep paper patient information in a secure location out of view of the public.
j. Ensure all non Baptist Health 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.
k. If there is any doubt or, in the case of shared rooms, ask the patient's permission before disclosing any PHI.

3. Technical Safeguards
   a. Protect your passwords and never share them, it may help if you safeguard your passwords the same way as you safeguard your personal ATM PIN, or banking information.
   b. Remember to ALWAYS log off your computer before walking away, even for a few minutes.
   c. When using a shared computer, you MUST Log off any clinical applications after accessing patient information.
   d. When faxing, ALWAYS use a cover sheet and confirm the fax number to ensure a safe transmission; as well as using a secure location for incoming faxes.
   e. Email communications containing any patient, financial or Baptist Health confidential information should remain within the Baptist Health/Bethesda email system. Ask your supervisor for further assistance if your job requires you to use email outside the Baptist Health email system.
   f. No personal electronic mobile devices should be used in patient care areas (BHSF HR Policy 6400).).
   g. 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.
   h. PHI may NEVER be shared, posted or otherwise disclosed on Social Media.
   i. You may never share, use, or disclose PHI in a Text Message using your personal phone.

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
- BHSF-74220-001.00 Unified Corporate Privacy Policy on HIPAA Compliance

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.