



POLICY TITLE: Access and Inspect - Patients Request for Access to Protected Health Information While In-house

Responsible Department: Corporate Privacy Office

Creation Date: 2003/06/24

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): 2021/12/14

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 grants patients important rights with respect to health information obtained and maintained by Baptist Health. The Baptist Health Privacy Office is responsible for ensuring the confidentiality of Baptist Health patient medical information and responding to such requests. Individuals who are inpatients have the right to review and inspect their medical information.

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.

Individuals who are inpatients have the right to review and inspect their medical information. This policy formalizes and defines the process of receiving and responding to patients request to access their Health Information during their hospitalization.

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*.

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.

- **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 grants patients important rights with respect to health information maintained by Baptist Health. Generally, upon first service delivery, the BHSF Notice of Privacy Practices is provided to patients to inform them of their rights, including the right to access and inspect their health information. Once a patient or patient personal representative expresses their desire to review the medical record during the hospitalization, All workforce members and individuals covered by this policy should follow the below guidelines to ensure patients are afforded their right to inspect their medical information.

1. Nursing Responsibilities
 - a. Assess the patient's capacity to make health care decisions.
 - b. Contact entity Patient Experience representative to visit the patient. If the request is made by the patient after regular business hours, inform the patient or the patient's personal representative that their request will be processed on the next business morning.
 - i. If the patient or the patient's personal representative is unable to wait until the next business morning for the request to be processed, escalate the request to appropriate BHSF leadership.
 - c. Attempt to clarify the reason for medical record review, such as, what part(s) of the medical record the patient is interested in reviewing; (e.g., lab results, imaging reports , consultation reports, etc.), and any specific concerns.
 - d. Inform the patient or the patient's personal representative that the medical record may not be complete and that their physician(s) will clarify any additional questions they have following their chart review.
 - e. If the nurse feels the information contained in the patient's medical record is of a sensitive nature or the care team may not have been discussed information available in the record with the patient, contact the patient's attending physician and request that they provide an order for a chart review by the patient/patient's personal representative.
 - i. If, in the physician's judgment, he/she feels that information contained in the medical record is of such a nature that it is not conducive to promoting the patient's therapeutic condition then the patient will be offered other alternatives, see 2a.
2. Patient Experience Responsibilities
 - a. Discuss alternatives with the patient or the patient's personal representative, such as a patient and family care conference or the release of pertinent medical records.
 - b. Complete and provide the patient with Form 6008 – Request to Examine Personal Medical Record.
 - c. If the patient lacks the capacity to make healthcare decisions, the patient's personal representative may submit the request to review the medical record by completing Form 6008 – Request to Examine Personal Medical Record.
 - i. Patient's personal representatives are individuals other than the patient who may request access to the medical record such as:
 - 1) The patient's designated surrogate
 - 2) A proxy appointed by the hospital
 - 3) A durable power of attorney for healthcare decisions

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.

- 4) Other legal representative
 - ii. The same procedures should be followed when accepting a request from the patient's personal representative as when accepting a request from the patient.
 - d. Notify the Corporate Privacy Office by telephone, (786) 598-8850 or email Privacy@BaptistHealth.net that a patient has requested to examine their medical record, and send the completed form for approval.
 - e. A Patient Experience representative or designee, in collaboration with the health care team (including Social Work, if necessary) should perform a preliminary screening of the medical record and notify the Privacy Office of any mitigating circumstances or the presence of criteria for denial.
 - f. A Patient Experience representative or designee shall notify the Privacy Office of the physician's recommendation and the Privacy Office, in collaboration with entity Risk Management shall determine if the request will be granted or denied.
 - g. A Patient Experience representative or designee shall notify the entity Risk Management department off any inpatients request for inpatient access.
3. Privacy Office/Risk Management Responsibilities
- a. The Privacy Office representative will grant or deny the requested access based on the following factors:
 - i. Presence of a Physician's Order. Absence of a physicians' order does not necessarily mean that the request will be automatically denied;
 - ii. The advice of Risk Management regarding access; and
 - iii. The recommendation of Patient Experience.

The Privacy Office may involve Risk Management to determine whether any of the following factors are present. The Chief Privacy Officer will make the final decision to grant or deny access.

 - a) Information could harm the patient: If the medical record relates to an emotionally disturbed patient or contains information about the patient's emotional state or any other sensitive information, a copy of the request and the relevant information shall be forwarded to the patient's attending physician, using the appropriate letter. If the physician recommends that the patient's request for access be denied and the patient requests a review of such denial, the denial must be reviewed in accordance with the applicable HIPAA privacy procedure.
 - b) Information references confidential sources: If the medical record or other designated record set prominently refers to a confidential source of the information, the request and the relevant information shall be forwarded to the patient's attending physician, using the appropriate letter. If the physician denies the patient's request for access and the patient requests a review of such denial, the denial must be reviewed in accordance with the applicable HIPAA privacy procedure.
 - c) Information regarding inmates: If the subject of the information is an inmate in a correctional institution, the request shall be forwarded to the warden of the applicable correctional institution, using the appropriate letter attached hereto. If the warden denies access, such denial is not subject to review.
 - d) Information regarding research: If the requested information is prominently marked as being restricted while research is still in progress, the request and the relevant information shall be forwarded to the Principal Investigator, using the appropriate letter attached hereto. If the Principal Investigator denies access, such denial is not subject to review.
 - b. If the Privacy Office denies a request, they will:
 - i. Document the denial on the Form 6008 - Request for Access to Medical Records; and
 - ii. Write a letter to the patient or the patient's personal representative explaining the grounds for the denial.
 - c. When a request is denied by the Privacy Office, the form is marked as denied and faxed or emailed to the Patient Experience Representative of the affected entity to provide to the patient or the patient's personal representative. If a partial denial is made, the portion(s) of the medical record which are excluded from review will be removed. A copy of the denial is placed in the medical record. Further inquiries from the patient or the patient's personal Representative are referred to the Privacy Office.

- d. If the Privacy Office approves a request for access for hospitalized patients, they will notify Patient Experience. The appropriate Patient Experience representative or designee will schedule a convenient time, not exceeding three business days from the request submission date, to meet with the patient or the patient's personal representative to review the record. In the event that the requesting patient is under isolation precautions, the request will be granted only when the medical condition is non-communicable or the safety precautions have been lifted.
 - i. For all inpatient reviews, the following conditions will apply:
 - 1) A time limit will be imposed by Patient Experience to be determined by Patient Experience leadership, based on the time needed to review the record.
 - 2) The Patient Experience representative or designee must be present during the review of the record to safeguard the integrity of the medical record.
 - 3) The Patient Experience representative or designee will not provide any interpretation of the medical record. The Patient Experience representative will provide the patient an opportunity to document or write down any questions to discuss with their treatment team.
 - 4) The patient or legal representative may have a member of the patient's immediate family present while he or she is reviewing their medical record, along with the Patient Experience representative or their designee.
 - 5) If the patient, personal representative or family member becomes disruptive during the review of the medical record, the record review will be terminated or the disruptive individual will be asked to leave.
- e. If the items that the patient wishes to review are not contained in the paper medical record, the Patient Experience representative or designee will provide an electronic chart review.
 - i. For electronic medical record inpatient reviews, the following conditions will apply:
 - 1) A time limit will be imposed by Patient Experience to be determined by Patient Experience leadership, based on the time needed to review the record.
 - 2) The Patient Experience representative or designee must be present during the review of the record to safeguard the integrity of the electronic medical record.
 - 3) The Patient Experience representative or designee will bring a computer into the patient's room, and log on to the hospital electronic information system to review the electronic Protected Health Information.
 - 4) No patients or patient's personal representatives or family members may utilize the computer. The review must be conducted by Patient Experience representative or designee using their own user name/password.
 - 5) The Patient Experience representative or designee will not provide any interpretation of the medical record. The Patient Experience representative will provide the patient an opportunity to document or write down any questions to discuss with their treatment team.
 - 6) The patient or legal representative may have a member of the patient's immediate family present while he or she is reviewing their medical record, along with the Patient Experience representative or their designee.
 - 7) If the patient, personal representative or family member becomes disruptive during the review of the medical record, the record review will be terminated or the disruptive individual will be asked to leave.

SUPPORTING/REFERENCE DOCUMENTATION:

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- Applicable Florida State Laws
- Corporate HIPAA Privacy Policies

RELATED POLICIES, PROCEDURES AND ASSOCIATED FORMS:

- 10000-74220-101.00 – Notice and Choice: Provision of the BHSF Notice of Privacy Practices

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.

- Form 0027 and 0027s – Notice of Privacy Practices Brochure
- Form 6008 and 6008s – Request to Examine Personal Medical Record

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’s South Florida’s Privacy Office in conjunction with Human Resources, as circumstances may dictate.