POLICY TITLE: 606.00 Information Blocking

Responsible Department: Corporate Privacy Office

Creation Date: 02/01/2021
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: Tony Ambrozie
Title: Senior Vice President and Chief Digital & Information Officer

APPROVED BY: Matthew Arsenault
Title: Executive Vice President & Chief Financial Officer

PUBLISHED (Released): 2021/12/15

SUMMARY & PURPOSE:

In response to concerns that some individuals and entities were engaging in practices that unreasonably limited the availability and use of electronic health information ("EHI") for authorized and permitted purposes, the federal government prohibited practices of "information blocking" unless an exception applies. Restrictions on information blocking primarily take two forms:

1. Health care providers must attest that they are not engaged in certain information blocking practices in order to satisfy the requirement of the Promoting Interoperability program (formerly known as the Medicare EHR Incentive program and more commonly known as the "Meaningful Use" program), which impacts Medicare reimbursement levels; and

2. Practices that constitute information blocking, as defined in the 21st Century Cures Act of 2016 and implementing regulations may result in other types of penalties (which vary based on the type of entity).

If a requester, whether a patient, health care provider, or other third party, requests EHI for an authorized and permitted purpose, the presumption is that Baptist Health will provide the requested access to EHI unless an exception applies (such as a privacy law prohibits the disclosure or there is a reasonable belief that providing the access will cause physical harm).

Accordingly, the following policy is intended to assist Baptist Health in preventing prohibited information blocking practices that may lead to penalties and reductions in reimbursement.

POLICY:

It is the policy of Baptist Health South Florida, Inc. ("BHSF" or "Baptist Health") to comply with applicable state and federal laws in a manner that supports its primary mission.

Baptist Health will not knowingly interfere with access, exchange, or use of EHI in violation of applicable laws and regulations unless the practice is required by law or a Regulatory Exception applies.

SCOPE/APPLICABILITY:

This policy applies to all Baptist Health employees and other persons

This policy applies to Baptist Health, its affiliates, all workforce members, and others as described below whose conduct, in the performance of work for Baptist Health, is under Baptist Health's direct control and that control or influence the access, exchange, or use of EHI..

- **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.

This policy applies to all of Baptist Health's EHI and to EHI that Baptist Health maintains on behalf of others.

1. Definitions

a. EHI.
   i. Until October 6, 2022, EHI includes all information in the most current version of the United States Core Data for Interoperability ("USCDI"), currently available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.
   ii. On and after October 6, 2022, EHI includes all electronic protected health information in a patient's designated record set maintained by or on behalf of Baptist Health, which includes:
      1) The medical records (e.g., the electronic medical record or electronic health record) and billing records about individuals maintained by or for Baptist Health; and
      2) 2) Any other electronic protected health information used in whole or in part by or for Baptist Health to make decisions about individuals (such as treatment or payment decisions).

b. Regulatory Exception. For purposes of this policy, a Regulatory Exception is an exception to information blocking set forth in 45 C.F.R. part 171. Examples of Regulatory Exceptions include:
   i. Certain practices to prevent physical harm to the patient or others;
   ii. Satisfying privacy law criteria (e.g., obtaining the patient's authorization or complying with a patient's requested restriction);

iii. Implementing appropriate security safeguards; or
iv. Where the request is infeasible.

c. Information Blocking Review Committee ("IRBC"). The IRBC is a multidisciplinary committee that has responsibility for overseeing and implementing practices and policies related to Information Blocking, as well as reviewing any requests for EHI pursuant to this Policy.

PROCEDURES TO ENSURE COMPLIANCE:

1. **Responsibility for Oversight of Prohibition on Information Blocking.** The BHSF Chief Privacy Officer, in conjunction with the Information Blocking Review Committee ("IBRC"), will have responsibility for overseeing and implementing practices to prohibit information blocking involving EHI.

2. **Training.**

   a. The IBRC will work with appropriate BHSF stakeholders to implement annual training of appropriate Workforce on the prohibition on information blocking and this Policy.
   b. Such training will focus on:
      i. Informing Workforce members that Baptist Health has a responsibility to generally allow access, exchange, and use of EHI to the extent permitted by law.
      ii. Explaining what constitutes EHI and information blocking.
      iii. Identifying common examples of prohibited information blocking practices.
      iv. Identifying, at a high level, some of the Regulatory Exceptions that may be applicable to Workforce (such as actions to prevent physical harm to the patient or other individuals).
      v. Instructing Workforce regarding how and to whom to report potential information blocking practices.

3. **Identification of Potential Information Blocking Practices.** The Chief Privacy Officer, in conjunction with the IBRC, will oversee a periodic review to identify practices that may constitute prohibited information blocking.

   a. To the extent feasible, a review will be conducted no less than every two years.

   b. Relevant stakeholders within Baptist Health will be interviewed to identify practices that potentially interfere with third parties' access, exchange, or use of EHI.

   c. For each practice that interferes with a third party's access, exchange, or use of EHI, the IRBC shall either:
      i. Document that the practice is required by law or a Regulatory Exception applies; or
      ii. Develop and implement a plan to remediate the practice.

4. **Patient Requests.**

   a. Automated Requests. BHSF shall make EHI available through a patient portal to patients and their chosen proxies without unreasonable delay unless a practice that interferes with or limits such access is required by law or falls within a Regulatory Exception.

b. Non-Automated Requests. To the extent that a patient or the patient's personal representative requests access to EHI, such as through the Health Information Management Department, the Health Information Management Department shall make EHI available to the patient or patient's personal representative without unreasonable delay, and ensure that any denial, delay, or cost in providing the access to EHI falls within a Regulatory Exception (See also, BHSF Privacy Policy 105 – Access of Individuals to Protected Health Information).

c. Example of a Prohibited Information Blocking Practice:
   i. Baptist Health will not deny or delay a patient's access to EHI, including lab results or sensitive diagnoses, based on a belief that the patient cannot emotionally handle the information or that the patient does not have the ability to understand the information. If a clinician believes that access to EHI would cause:
      1) physical harm to the patient or someone else;
      2) emotional harm to another person that is referenced in the EHI; or
      3) the request is from the patient's personal representative and providing the EHI to the personal representative likely would cause substantial harm to the patient,

   Then the clinician should promptly notify the Chief Privacy Officer at privacy@baptisthealth.net or call 786-596-8850.

5. Contracting. Supply Chain Leadership will coordinate with Information Blocking Review Committee (IBRC) to:

a. Review new contracts involving EHI to verify that they do not involve prohibited information blocking; and

b. Implement a system so that new contracts involving EHI do not involve prohibited information blocking.

6. Application Programming Interface (API) Requests.

a. Information Blocking Review Committee (IBRC) will coordinate with the Baptist Health Technology & Digital Department to make EHI available to third parties through an API for permitted and authorized purposes to the extent not limited by A Regulatory Exception, and as may be required under Medicare's Promoting Interoperability program (also known as the "Meaningful Use" program), including that:
   i. Information necessary for connecting to Baptist Health's API(s) is reasonably available; and
   ii. Access to the API(s) is not denied, delayed, or otherwise interfered with unless a Regulatory Exception applies.

7. Third-Party Requests.

a. Third party requests (non-patient requests) for EHI received by a BHSF Workforce member should be submitted for review to the IBRC at InfoBlocking@Baptisthealth.net.

b. Information Blocking Review Committee (IBRC) should coordinate with appropriate stakeholders to ensure that all third-party requests for EHI for permitted and authorized purposes are granted without unreasonable delay or cost unless a Regulatory Exception applies.

8. Actions as a Health Information Exchange

a. The IRBC will identify whether BHSF controls or influences EHI of others as a health information exchange/network ("HIE").

b. To the extent that BHSF controls or influences EHI of others as an HIE, the IRBC will coordinate with appropriate stakeholders to not interfere with access, exchange, or use of others' EHI in its role as an HIE unless the practice is required by law or a Regulatory Exception applies.

c. The Supply Chain Department will coordinate with the BHSF Legal Department and BHSF Technology & Digital Department to review contracts involving Baptist Health acting as an HIE to ensure that such contracts do not include terms that impermissibly constitute information blocking.

9. Reporting Potential Information Blocking Practices.

a. Any Workforce member who learns of a practice that interferes with a third party's access, exchange, or use of EHI should immediately report the practice to the Information Blocking Review Committee (IBRC) at DG-COInfoBlockingReviewCommittee@baptisthealth.net, unless the Workforce member knows that the Information Blocking Review Committee (IBRC) has already analyzed and approved the practice.

10. Promoting Interoperability Program (Meaningful Use)

a. Regulatory Analytics Manager will coordinate with the Chief Data Officer to identify when Baptist Health will attest to not information blocking as part of the Medicare Promoting Interoperability program.

b. Immediately prior to BHSF's annual attestation in the Promoting Interoperability program, Regulatory Analytics Manager will confirm to Chief Data Officer that they are not aware of any ongoing information blocking practices that are inconsistent with the Promoting Interoperability program's information blocking attestations.

11. Documentation Retention.

a. The Information Blocking Review Committee (IBRC) will retain all documentation indicating that practices are not information blocking for a minimum of six years from when the practice was last in effect.

SUPPORTING/REFERENCE DOCUMENTATION:

- 45 C.F.R. part 171 (prohibition on information blocking pursuant to the 21st Century Cures Act)
- 42 C.F.R. § 495.40(a)(1)(I) and (b)(1)(I) (information blocking attestation requirements for the Medicare Promoting Interoperability program)

RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:

- Corporate HIPAA Privacy Policies
- Applicable Technology and Digital Policies

ENFORCEMENT & SANCTIONS:

Enforcement of this policy is the responsibility of the Information Blocking Review Committee, HIPAA Privacy Office and the appropriate Human Resources area.