POLICY TITLE: 603.00 Auditing and Monitoring Electronic Protected Health Information Access and Activity

Responsible Department: Corporate Privacy Office

Creation Date: 11/04/2015
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 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.

Compliance with state and federal regulations require the implementation of procedures to routinely review records of system activity such as audit logs, access to ePHI reports, and activity of user reports in information systems that contain or use ePHI.

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.

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. This policy supports the process by which the Privacy Office will audit and monitor access and user activity of Electronic Protected Health Information (ePHI) by members of the workforce and users granted access to the organization's ePHI.

SCOPE/APPLICABILITY:
This policy applies to Baptist Health personnel charged with implementing the federal privacy regulations under HIPAA.

AUDIT PROGRAM

1. To ensure on-going compliance with the Rule, the Corporate Privacy Office has developed an Audit Program "the Program". The overall purpose of the Program is to ensure regulatory compliance by validating;
   a. Patients afforded their privacy rights under HIPAA; and
   b. If BHSF workforce is accessing, using, and disclosing protected health information ("PHI") for Treatment, Payment and Health Care Operations, "TPO").
2. The privacy office conducts audits and investigations in many areas including those considered to be "high risk" to BHSF or patients or which are the subject of an incident and/or complaint reported to the Privacy Office. The Program validates compliance through a variety of proactive and reactive audits. The Program and audits ensure that sensitive information entrusted to BHSF is safeguarded.
3. The Annual HIPAA Audit Plan will vary from year to year and should consider appropriate risk factors.

PROCEDURES TO ENSURE COMPLIANCE:

Baptist Health will audit and monitor access and user activity of Electronic Protected Health Information (ePHI) by members of the workforce and users granted access to the organization's ePHI. The department uses various audit tools and audit logs to perform audits. The frequency, types of reports, and scope of reports for the audits are outlined on Annual HIPAA Audit Plan. Documentation shall be retained in accordance with the organization's document retention policy.

1. General Requirements
   a. Members of the workforce, Business Associates, and users granted access to the organization's PHI may only use or disclose ePHI as related to performing job responsibilities.
   b. Unauthorized review, duplication, printing, dissemination, removal, publish, faxing, modification of ePHI within the EHR, or other property of the organization or improper use of information obtained by unauthorized means is grounds for Sanctions.
   c. All authorized users are granted a unique user name and password to access the organization's ePHI.
   d. All authorized ePHI users receive job specific education and training to include: appropriate ePHI activity, unauthorized activity, sanctions, job responsibilities, and reporting requirements.
2. Type and Frequency of Audit Reports and Monitoring Activities
   a. Systems containing ePHI with audit capabilities should be audited in accordance with the Annual HIPAA Audit Plan.
   b. Audit activities may be categorized as:
      i. Standard - Report is scheduled to run on a fixed schedule (e.g., weekly, monthly, quarterly). Periodicity shall be based on the risk to the organization and determined by the Privacy Office.
      ii. Nonstandard - Reports are not scheduled to run periodically and can be used to audit a non-critical policy.
      iii. Ad Hoc - Reports are run in response to an inquiry, question, complaint or investigation.
3. Reporting and use of audit results
   a. A summary of ePHI Auditing and Monitoring activities is reported by the Privacy Office on a monthly basis.
   b. The Privacy Officer will submit an annual report to the appropriate committee (i.e., Privacy/Security Review Board) on audit trends specific to location, department, person or process.
   c. Trending information from audits will be reviewed and used to update workforce education materials.
4. Complaint-driven or ad hoc audits
   a. Complaint-driven audits will be conducted as soon as possible after the complaint is received.
   b. Requests for audit data will be generated as appropriate.
5. Annual HIPAA Audit Plan
   a. If applicable, during the quarter preceding the upcoming fiscal year, the annual HIPAA Audit Plan shall be submitted by the Privacy Officer to the appropriate committee for approval.
6. Retention:
   a. The Privacy Office will retain no more than three (3) rolling calendar years of audit data for privacy monitoring purposes.

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
- Corporate HIPAA Audit Plan

ENFORCEMENT & SANCTIONS:

Enforcement of this policy is the responsibility of the Corporate Privacy Office.