Baptist Health South Florida

POLICY NO.: 10000-74220-701.00
TYPE: Administrative

POLICY TITLE: 701.00 Privacy and Security Incident Reporting and Response

Responsible Department: Corporate Privacy Office

Creation Date: 12/03/2005
Review Date: 2021/12/10
Revision Date: 2021/12/10

SUBMITTED BY (AUTHOR): Mercedes del Rey
Title: Assistant Vice President, Chief Privacy Officer

APPROVED BY: Anthony Longo
Title: Vice President**,** Chief Information Security 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:

To summarize Baptist Health South Florida, Inc.'s ("BHSF" or "Baptist Health") methods for reporting privacy and/or security incidents or activities that pose a threat to the privacy and/or security of the organizations' employees and patients' protected health information ("PHI") or other personally identifiable information ("PII") or other sensitive, nonpublic information entrusted to the organization's care. Both state and federal law govern this policy. Consistent with applicable laws, BHSF protects the sensitive information entrusted to its care, responds to incidents related to PHI and PII, and takes reasonable steps to mitigate any harmful effects expected to result from any use or disclosure of sensitive information that varies from uses and disclosures permitted by law.

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/or personally identifiable information. It is BHSF's 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. Baptist Health's policy is to adhere to both the Health Insurance Portability and Accountability Act of 1996 as amended from time to time and including any regulations promulgated thereunder (collectively, "HIPAA") as well as the Florida Statute §501.171 ("Security of Confidential Personal Information"), as well as any other applicable state or federal laws (hereinafter, HIPAA, the Florida Security of Confidential Personal Information Law, and any other applicable state or federal laws are collectively referred to as "Applicable Laws"). This is the policy to be used in conjunction with the BHSF Privacy and Security Incident Response Plan.

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.

There are no exemptions to this policy.

DEFINITIONS:

1. **Protected Health Information (PHI):** includes any health information (including information that merely identifies an individual as a current or former patient of BHSF) unless the health information has been appropriately de-identified.
2. **Personally Identifiable Information (PII):** information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
3. **Privacy Incident:** a privacy incident is "a suspected or confirmed incident involving PHI or PII." A privacy incident is an adverse event or action that is unplanned, unusual, and unwanted that happened as a result of non-compliance with Baptist Health's privacy policies. It must pertain to the unauthorized access, use or disclosure of PHI or PHI including "accidental disclosure" such as misdirected e-mails or faxes.
4. **Security Incident:** "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."
5. **Security Threat**: any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
6. **Breach:** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. (Note: The definition of "breach" applies with regard to the HIPAA Privacy Rule.

PROCEDURES TO ENSURE COMPLIANCE:

For purposes of this policy, "incident" includes both privacy and/or security incidents and other incidents which may constitute a breach under federal or state law.

1. To illustrate, some (but not all), examples of the type of privacy and/or security incidents to which this Plan applies include:
   a. Orally sharing a patient's information to an unauthorized third party;
   b. Disclosure of PHI, including paper disclosure, or PII by email or fax release, or inadvertent posting of data on a website;
   c. Workforce member accessing PHI or PII for information about co-workers, friends, or family members out of curiosity, i.e., without a medical or business-related purpose;

d. Intentional and non-work related access by staff member of neighbor's health information;
e. Misdirected FAX of PHI to the incorrect patient;
f. Misdirected FAX of PHI to a local business instead of the requesting provider's FAX;
g. Discharge documents of one patient given to another patient;
h. Prescription document intended for Patient #1 given to Patient #2;
i. Billing or credit card information of Patient #1 sent to Patient #2;
j. Briefcase containing patient information stolen from auto;
k. Loss or theft of removable media or device such as Laptop, Smartphone, USB/thumb drive/memory stick containing PHI or PII patient data, patient-identifying photos or other PHI;
l. FAX or email containing PHI or PII sent to the incorrect recipient Discharge documents of one patient provided to another patient;
m. Medical record documents left unattended in cafeteria;
n. Explanation of Benefits (EOB) sent to the wrong entity;
o. Papers containing protected health information found scattered along the roadside;
p. Medical records or other PHI lost in mailing process and never received;
q. Disclosure of PHI or patient images on the internet, social media, to the media, or on any other public forum without authorization;
r. An attack to our applications or technical systems:
    i. executed from removable media, such as a flash drive or disk, or a peripheral device;
    ii. that employs brute force methods to compromise, degrade, or destroy systems, networks, or services;
    iii. executed from a website or web-based application; or
    iv. executed via an email message or attachment;
s. Unauthorized Access - Logical or physical access was gained to a network, system, application, data, or other resource by a person or persons not authorized to have access to the resources;
t. Denial of Service - An attack occurred that resulted in the prevention or impairment of the authorized use of networks, systems, or applications;
u. Malicious Code – A network, system, application or other resource was infected by a virus, worm, Trojan horse, or other code-based malicious entity causing a destruction of information or interference with information system operations;
v. Inappropriate Usage – A person or persons have violated acceptable computing use policies;
w. Compromised Credentials – if you think that your BHSF user name(s) or password(s) are being used by someone else.

2. Incident Reporting Methods
    a. Breach notification will be carried out in compliance with Applicable Laws.
    b. Workforce Responsibilities:
        i. BHSF maintains scalable processes designed to respond to various types of incidents. Every BHSF workforce member is responsible for reporting immediately any suspected or known privacy and/or security incidents and/or breaches of the privacy or security of PHI or PII.
        ii. There are a variety of methods and/or channels for reporting incidents. BHSF will maintain a variety of methods to allow employees as well as third parties, including vendors and contractors, to report suspected incidents in which the confidentiality, availability and/or integrity of patient information is compromised.
        iii. Key channels for reporting incidents include, but are not limited to the below:
            1) HIPAA Privacy Office / BHSF HIPAA Hotline
            2) BHSF Information Technology (IT) CTT or Systems Security
            3) Any BHSF supervisor or leader
            4) BHSF corporate compliance hotline or online (on BHSF intranet)
            5) BHSF Midas online Risk Management incident reporting system
            6) BHSF Patient & Guest Services
            7) BHSF Human Resources.

iv. Any BHSF supervisor or leader, or employee of Patient Experience, Human Resources, or any other department that becomes aware of a suspected incident shall immediately notify the Chief Privacy Officer ("CPO") or the Chief Information Security Officer ("CISO").

c. Referral to the Chief Privacy Officer ("CPO") or the Chief Information Security Officer ("CISO").
   i. All reported privacy/security incidents will be referred to the Chief Privacy Officer ("CPO") and/or in appropriate cases, to the Chief Information Security Officer ("CISO") for investigation.
   ii. The CPO and/or CISO will establish a process to review and assess all reported incidents.
   iii. The CPO and/or CISO will determine whether the Privacy/Security Incident Response ("IR") Plan must be activated.

d. Conducting a HIPAA Breach Risk Assessment and Documentation:
   i. Following receipt of notice of a privacy and/or security incident that involves PHI, BHSF shall conduct a risk assessment pursuant to Applicable Laws using the BHSF Breach Incident Risk Assessment Tool ("BRAT") to determine whether a breach has occurred.

e. Determination of Whether Notification is Required:
   i. For a breach of PII that also involves PHI, BHSF will treat the incident as a Breach of PHI and provide notifications in accordance with HIPAA.
   ii. For a breach of PII that does not involve PHI, BHSF will provide notification in accordance with the Florida Security of Confidential Personal Information Law.

f. Workforce Training:
   i. BHSF shall train all members of its workforce on the policies and procedures with respect to PHI and PII as necessary and appropriate for the members to carry out their job responsibilities.
   ii. Workforce training includes awareness level training on each member's responsibility to report privacy and/or security incidents.
   iii. Workforce training will be carried out in accordance with BHSF Privacy Policy 10000-74220-602.10 Compliance and Implementation - Privacy Training of BHSF Workforce and BHSF IT Policy 138 Security Awareness Training.

g. Privacy and/or Security Complaints:
   i. BHSF provides a process for individuals to make complaints concerning BHSF's privacy and/or security policies, procedures, compliance with such policies and procedures and the security of their information.
   ii. All such complaints must be reported to the CPO or CISO who will investigate the complaint and ensure complaints will be received and followed up on in accordance with BHSF Policy.

h. Sanctions:
   i. BHSF has in place and applies appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.
   ii. Sanctions will be applied in accordance with BHSF Privacy Policy 10000-74220-605.20 Compliance and Implementation - Sanctions for Privacy Violations.

i. Retaliation/Waiver:
   i. Individuals have the right to complain about concerns surrounding the access, use, disclosure and security of their information without fear of retaliation.
   ii. Individuals have the right to complain about concerns surrounding the access, use, disclosure and security of Baptist Health's information without fear of retaliation.
   iii. BHSF does not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. BHSF does not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

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")
- Florida Statute §501.171 ("Security of Confidential Personal Information")

RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:

- 10000-74220-001.00 Unified Corporate Privacy Policy on HIPAA Compliance
- 10000-74220-108.00 Patient Rights – Receiving and Responding to Privacy Complaints
- 10000-74220-602.10 Compliance and Implementation - Privacy Training of BHSF Workforce
- 10000-74220-605.20 Compliance and Implementation - Sanctions for Privacy Violations
- Information Technology 138 - Security Awareness Training.
- Information Technology 159 - Unified Corporate Policy for Compliance with the HIPAA Security Rule
- Privacy/Security Incident Response Plan
- Breach Risk Assessment Tool (BRAT)

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.