BAPTIST HEALTH POLICY AND PROCEDURE MANUAL No. 6.6.2		
Section: Privacy	**Subject:** PATIENT PRIVACY – PRIVACY VIOLATIONS	
Original Date: February 2008	**Supersede:** December 2017	**Effective Date:** November 2020
Review Date: November 2023	**Scope:** BAPTIST HEALTH	
Approved:	**/Brett S. McClung, CEO**	

I. POLICY

It is the policy of Baptist Health and its subsidiaries (collectively, "BH") to take appropriate steps to deter, investigate and correct violations of patient privacy.

II. PURPOSE

A. To ensure that BH has reasonable procedures in place to investigate, analyze, address, mitigate and correct violations of patient privacy utilizing the principles of a Collaborative Culture of Safety.

B. Our purpose in adopting a Collaborative Culture of Safety at Baptist Health is to support our core organizational values through continuous improvements in our culture; proactively managing risk within our organization; improving quality and reliability. The Systems and Behaviors Response Guide is an operational tool to apply these principles reliably.

C. To comply with Federal regulations.

D. To apply appropriate sanctions for violations in a consistent manner.

III. DEFINITIONS

BH Health Information Security Officer ("HISO"): BH's VP of Information Services or his designee(s). The BH HISO has the responsibility for oversight of BH's information security policies and BH's compliance with HIPAA security standards.

BH Privacy Officer: BH's Vice President of Risk Management, Patient Safety and Privacy or his designee(s). The BH Privacy Officer has the responsibility for oversight of BH's privacy policies and BH's compliance with applicable patient privacy law.

Business Associate: A person (other than a BH team member) or entity (other than a BH subsidiary) that, on behalf of BH, performs or assists in the performance of a function or activity involving the use or disclosure of IIHI, including claims processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing or the provision of legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

Electronic Protected Health Information ("EPHI"): Individually identifiable health information ("IIHI") that is transmitted or maintained in electronic form or media (e.g., stored on computer hard drives, network drives, computer discs, diskettes, optical disks and digital memory cards and information transmitted by e-mail systems and voicemail systems).

Individually Identifiable Health Information ("IIHI"): Information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   a. That identifies the individual; or
   b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Medical Executive Committee ("MEC"): A committee of medical staff officers and department chairpersons for a given BH hospital which has as one of its duties the responsibility of receiving, reviewing and taking necessary action on matters involving professional competence, professional conduct, ethics or violation of medical staff by-laws.

Protected Health Information ("PHI"): Any IIHI that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Need to Know Basis: A BH rule that BH team members, business associates or professional appointees are only permitted to obtain from a medical record or other source of IIHI the minimum amount of information necessary to accomplish the duties and responsibilities of their position.

IV. PROCEDURES

A. BH team members and Business Associates are responsible for reporting to the BH Privacy Officer, via the HIPAA Privacy Hotline (202-HIPA), any known or suspected violation of patient privacy by a BH team member, Business Associate or professional appointee.

B. BH has implemented reasonable measures and may implement additional such measures, under the supervision of the BH Health Information Security Officer, to document and audit access to each computer system containing EPHI regarding BH's patients. (For further detail, see *Patient Information Security – Login Monitoring*, BH Policy No. 4.13; see also *Patient Information Security – Activity and Audit Control Procedure*, BH Policy No. 4.14).

C. The manager of the department involved in a privacy concern is responsible for investigating, evaluating and applying the principles of Collaborative Culture of Safety to identify any system failures and/or behaviors contributing to the event. The results of the review will be forwarded to the BH Privacy Officer or designee(s) and the Collaborative Review Team, as necessary for disciplinary actions. (For further detail, see *Collaborative Culture of Safety*, BH Policy 2.37)

D. Upon report of a possible violation of patient privacy to the privacy office, the BH Privacy Officer or his designee(s) will review the report to determine if further investigation is warranted, if a breach has occurred and if the event meets the Department of Health and Human Services and/or Florida Statute requirement for notification.

E. If an investigation confirms that a BH team member has violated patient privacy, the violation and risk will be mitigated according to the Collaborative Culture of Safety policy and procedure. BH may also be required to report professionals who violate patient privacy to their respective licensing board depending on the gravity of the violation. (For further detail, see *Collaborative Culture of Safety*, BH Policy 2.37)

If it is determined that a member of the medical staff has violated patient privacy, a letter will be sent to the medical staff member and copied to the medical staff office. (For further action, refer to Medical Staff Discipline Policy No. 10)

The Privacy Office will collaborate with the Business Associate or other Covered Entity (involved in a privacy violation) to address privacy violations, reporting and risk mitigation strategies.

F. Examples of privacy violations include, but are not limited to the following:

1. Discussing IIHI in public when reasonably avoidable and not necessary for quick, effective and high quality patient care

2. Carelessness in handling IIHI (for example: faxing to wrong fax number, handing patient wrong records, prescriptions, etc.)

3. Releasing or disclosing IIHI without reasonable assurance that the authorization is proper

4. Failing to ensure that IIHI is properly secured:

    a. Failure to log off a computer in a non-secured location if EPHI may be accessed by it

    b. Leaving IIHI unattended in a non-secured location

    c. Failure to utilize locks and other available security devices

5. Inappropriate use of a computer account:

    a. Utilizing another's user name and password to access EPHI

    b. Allowing another person to access EPHI via one's own user name and password

6. Disclosing IIHI to another BH team member when one knows that such team member does not have a Need to Know about such IIHI

7. Accessing IIHI without a Need to Know if such access is without an intent to harm another person or to achieve personal gain (for example: accessing child's records)

8. Altering or tampering with any record containing IIHI

9. Any other inappropriate use, disclosure or accessing, of IIHI of any patient with intent to harm another person or to achieve personal gain.

10. No adverse action, including but not limited to threatening, intimidating, coercing, harassing, discriminating against, or taking any other retaliatory action against any individual or other person for filing of a complaint, testifying, assisting or participating in an investigation under 45 C.F.R. § 160.316 will be allowed by Baptist Health.

G. Baptist Health reserves the right to modify the level of progressive disciplinary action for its team members (up to and including termination) based upon mitigating and aggravating factors and the seriousness of the violation of patient privacy. Mitigating and aggravating factors, including, but not limited to, the following shall be taken into account when determining the severity of sanctions for the violation of patient privacy by a team member:

1. Nature and extent of IIHI involved;
2. Unauthorized user or recipient of IIHI;
3. Whether IIHI was actually acquired or viewed;
4. Extent to which risk to IIHI was mitigated;
5. Intent behind inappropriate use, disclosure or access;
6. Likelihood of harm to patient;
7. Number and gravity of prior privacy violations;
8. Number and gravity of other prior violations of BH code of conduct;
9. Prior awards or commendations; and
10. Prior employment performance in general.

V. REFERENCE/CROSS REFERENCES

A. References

Health Insurance Portability Act of 1996, (HIPAA)

B. Cross-references

Limitations on EMR Access by Team members, BH Policy No. 6.5.8
Immediate Discharge, BH Policy No. 1.2.10
Patient Information Security – Login Monitoring, BH Policy No. 4.13
Patient Information Security – Activity and Audit Control Procedure, BH Policy No. 4.14
Patient Privacy – Business Associate Agreements, BH Policy No. 6.5.6
Patient Privacy – Notice of Privacy Practices, BH Policy No. 6.5.2
Patient Privacy – Protection of Patient Information, BH Policy No. 6.5.1
Patient Privacy – Restriction of Patient Information & Confidential Communications, BH Policy No. 6.5.7
Patient Privacy – Use and Disclosure of Patient Information, BH Policy No. 6.5.3
Progressive Discipline, BH Policy No. 1.2.11
Collaborative Culture of Safety, BH Policy No. 2.37
Medical Staff – Disruptive Behavior, Medical Staff policy and Procedure Manual No. 10
Department of Health and Human Services, 45 C.F.R. § 160.316

This policy/procedure is only intended to serve as a general guideline to assist staff in the delivery of patient care; it does not create standard(s) of care or standard(s) of practice. The final decision(s) as to patient management shall be based on the professional judgment of the health care provider(s) involved with the patient, taking into account the circumstances at that time. Any references are to sources, some parts of which were reviewed in connection with formulation of the policy/procedure. The references are not adopted in whole or in part by the hospital(s).