Origination:	*09/2009*
Effective:	*08/2021*
Last Reviewed:	*08/2021*
Last Revised:	*08/2021*
Next Review:	*08/2023*
Sponsor:	*Leslie Hernandez: DIR, PRIVACY & DATA*
Section:	*GA-Corporate Compliance*
Manuals:	*Compliance*

GA-004-115 Notification to Affected Individuals of a Breach of Unsecured PHI

I. **Purpose**

The purpose of this policy is to facilitate a consistent approach to ensure North Broward Hospital District d/b/a Broward Health complies with Breach notification requirements concerning confidential information that is accessed, acquired, used, or disclosed without authorization. Specifically, the purpose of this policy is to adhere to the requirements of the Health Insurance Portability and Accountability Act (HIPAA), HIPAA Breach Notification Rule, Florida Information Protection Act (FIPA) and all applicable federal and state laws and regulations.

II. **Definitions**

A. **Breach**: a Breach means the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted under the Privacy or Security Rules, which compromises the security or privacy of the PHI.

B. **Breach of Security**: Unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent does not constitute a Breach of Security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

C. **Discovery Date**: The first day on which a Breach is known or should have been known to Broward Health.

D. **Occurrence Date**: The date which the privacy or security incident took place.

E. **Protected Health Information (PHI)**: Protected Health Information means individually identifiable health information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.
(2) Protected health information excludes individually identifiable health information:
(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) In employment records held by a covered entity in its role as employer; and
(iv) Regarding a person who has been deceased for more than 50 years.

F. **Personal Information (PI)**: Personal information means either of the following:

1. An individual's first name, or first initial and last name in combination with any one or more of the following data elements for that individual:
    a. A Social Security Number;
    b. A driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
    c. A financial account number or credit or debit card number, in combination with any required security code, access code or password that is necessary to permit access to an individual's financial account;
    d. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
    e. Any individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

G. **Unsecured PHI**: Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of the Health and Human Services (HHS).

H. **Workforce Members**: Workforce Member means any employee, independent contractor, agent, trainee, or other person who performs work for or on behalf of Broward Health. This includes full-time, part-time, and pool employees; associates; directors; officers; managers; supervisors; members of the Board of Commissioners and members of standing committees; medical staff employed by or otherwise affiliated with Broward Health; medical students and all other affiliated students or others receiving training at any Broward Health facility; and others who provide goods or services to Broward Health.

III. Policy

It is the policy of Broward Health to notify the affected individuals and appropriate authorities whenever PHI maintained by Broward Health or a Business Associate has been accessed, acquired, used, or disclosed without authorization in violation of applicable federal and state laws and regulations pertaining to privacy, security, and Breach reporting. Broward Health will notify the patient(s) or affected individual(s) as soon as possible, but no later than sixty (60) days, following the Discovery Date of the Breach.
If Broward Health has determined a Breach of Security, as defined by the Florida Information Protection Act (FIPA), has occurred, Broward Health's policy is to notify the patient(s), or affected individual(s), as soon as possible, but no later than thirty (30) days, after the Discovery Date of the Breach of Security. In order to ensure that Broward Health complies with its reporting obligations, Broward Health requires all Workforce Members or Business Associates to report any suspected or confirmed Breach of PHI or PI either directly to their Supervisor or Department Manager or the Broward Health Corporate Compliance & Ethics Department as soon as possible. Failure of any Workforce Member or Business Associate to comply with this policy may subject that Workforce Member or Business Associate to disciplinary action or penalties stipulated by contractual agreement.

IV. Procedure

A. Investigation

Once Broward Health's Compliance & Ethics Department receives notification that a potential

privacy/security incident has occurred, the Compliance & Ethics Department will undertake an investigation to assess if a Breach has occurred that mandates reporting the incident to the affected individual(s), the United Stated Department of Health and Human Services (HHS), the Florida Department of Legal Affairs and the media (if applicable based on the circumstances of the Breach). The Compliance &Ethics Department will document the findings of its investigation and take necessary steps to address any Breach as defined by HIPAA, FIPA or other applicable laws.

1. To determine if a Breach has occurred, the Chief Compliance/Privacy Officer, or designee shall apply and document a three-step analysis in which it must determine the following:
    a. Whether there has been an acquisition, access, use, or disclosure of PHI that is not permitted under the HIPAA privacy regulations (the Privacy Rule) or FIPA.
    b. An acquisition, access, use, or disclosure of PHI is presumed to be a Breach unless Broward Health or its Business Associate demonstrates a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
        i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
        ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
        iii. Whether the protected health information was actually acquired or viewed; and
        iv. The extent to which the risk to the protected health information has been mitigated.
    c. Whether the incident falls within one of the following three limited exceptions to the definition of Breach:
        i. Any unintentional access, use, or disclosure of PHI by a covered entity's or business associate's workforce member or person acting under the authority thereof, if such access was in good faith, within that person's scope of authority, and did not result in further impermissible use or disclosure of the PHI;
        ii. Any inadvertent disclosure by a person who is authorized to have access to such PHI to another authorized person at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the PHI disclosed is not further used or disclosed in an impermissible manner;
        iii. Disclosure of the PHI where the covered entity or business associate has a good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain the PHI.
2. The covered entity or business associate bears the burden of proof regarding whether a Breach has occurred. It is important that the risk assessment processes and the considerations supporting those determinations are effectively documented. The risk assessment process will be completed for all impermissible uses or disclosures regardless of the type (i.e, paper, verbal, electronic).

B. **Patient Notification**

    a. After a complete investigation, and without unreasonable delay but in no case later than sixty (60) days from the Breach discovery, unless otherwise provided by federal laws and regulations, the Compliance &Ethics Department will facilitate written notice to the patient or:

i. If the patient is deceased, the next of kin or personal representative.

ii. If the patient is incapacitated/incompetent, the personal representative.

iii. If the patient is a minor, the parent or guardian.

b. If the complete investigation confirms that the Breach has compromised the security of a computerized data system, notification must be made to all individuals whose PI is, or is reasonably believed to have been accessed, acquired, disclosed, or used by an unauthorized individual. Notification must be made without unreasonable delay and in no case later than thirty (30) days in accordance with FIPA.

c. Written notification must be sent to the last known address of the patient or next of kin.

d. In the case where there is insufficient or out-of-date contact information:

i. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as a telephone call.

ii. In the case that there are ten (10) or more individuals for which there is insufficient or out of date contact information and contact information is not obtained, the facility shall post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside.

e. In any case deemed urgent because of possible imminent misuse of Unsecured PHI, Broward Health may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.

f. Provide notice in major print or broadcast media in the geographic area where a patient can learn whether or not his/her Unsecured PHI is possibly included in the Breach. A toll-free number must be included in the notice.

C. **Media Notification**

a. In the case where a single Breach event affected more than five hundred (500) residents of the same State or jurisdiction, notice shall be provided to prominent media outlets. A jurisdiction is defined as a geographic area smaller than a state (e.g., city, county).

b. The Chief Compliance/Privacy Officer, or designee will work with the Broward Health Corporate Communications and Marketing Department as well as the Broward Health General Counsel's Office to coordinate this notification as required.

D. **HHS Notification**

a. Notice should be provided by the Chief Compliance/Privacy Officer or designee, contemporaneously with individual notice, to the Secretary of the Department of Health and Human Services (HHS) immediately, without unreasonable delay and no later than sixty (60) days from the Discovery Date of the Breach, of an event impacting five hundred (500) or more individuals.

b. If a Breach has occurred but affects less than five hundred (500) individuals, the Compliance & Ethics Department shall maintain a log of any such Breach discovered that year and annually submit the log to HHS no later than 60 days after the end of the calendar year.

E. **Content of Notification**

a. Regardless of the method by which the notice is provided to patients, the Chief Compliance/

Privacy Officer will ensure the notification is in plain language and includes, at a minimum:

i. A brief description of what happened, including the date of the Breach and the Discovery Date of the Breach, if known.

ii. A description of the types of Unsecured PHI that were involved in the Breach, such as full name, Social Security Number, date of birth, home address, account number, or treatment information. Only generic descriptions should be listed in the notice (i.e., date of birth rather than the patient's actual birth date).

iii. The steps the individual should take to protect themselves from potential harm resulting from the Breach.

iv. A brief description of what the covered entity is doing to investigate the Breach, mitigate harm to the individual, and to protect against any further Breaches.

v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

F. **Notice to Florida Department of Legal Affairs (FIPA)**

a. Notice should be provided to the Florida Department of Legal Affairs in the event of a Breach affecting five hundred (500) or more individuals in accordance with FIPA. Such notice will be provided by the Broward Health Compliance & Ethics Department without unreasonable delay, but no later than thirty (30) days from the Breach Discovery Date.

b. Notice to the Florida Department of Legal Affairs will include:

i. A synopsis of the events surrounding the Breach at the time notice is provided.

ii. The number of individuals in Florida who were or potentially have been affected by the Breach.

iii. Any services related to the Breach being offered or scheduled to be offered, without charge, by Broward Health to individuals, and instructions as to how to use such services.

iv. A copy of the notice to individuals.

v. The contact information of the Compliance &Ethics Department from whom additional information may be obtained about the Breach.

c. Upon the request of the Florida Department of Legal Affairs, Broward Health will provide:

i. A police report, incident report, or computer forensics report.

ii. A copy of the policies in places regarding Breaches.

iii. Steps that have been taken to mitigate the Breach.

G. **Notice to Credit Reporting Agencies** (FIPA)

a. In the event a Breach of Security affects 1,000 individuals, then notice shall be provided to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p) of the timing, distribution, and content of the notices.

b. If a law enforcement official provides a written statement that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, and the statement specifies the time for which a delay is required, Broward Health must delay such notification, notice, or posting for the time period specified in the statement.

V. **Enforcement**

All Workforce Members whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy will be subject to appropriate remedial and/or disciplinary action, up to and including termination of any employment or other relationship, in accordance with the GA-004-160 Sanctions for Non-Compliance with Information Privacy and Security Policies.

VI. **Document Retention**

Broward Health will retain all documents relating to this policy for a period as defined in GA-004-135 Record, Retention, Storage and Disposal.

VII. **Exceptions**

There are no exceptions to this Policy.

VIII. **Interpretation and Administration of this Policy.**

This Policy shall be assessed and updated at least bi-annually (and more frequently, if appropriate) and reviewed as necessary. Within 30 days of the effective date of any revisions or additions to this Policy, a description of the revisions shall be communicated to all affected responsible persons at Broward Health and a copy of the revised Policy shall be made available. The Chief Compliance and Privacy Officer will monitor Broward Health's adherence to this Policy.

Administration and interpretation of this Policy is the responsibility of the Chief Compliance and Privacy Officer.

IX. **Related Policies**

A. GA-004-015 Business Associates Agreements

B. GA-004-160 Sanctions for Non-Compliance with Privacy & Security Policies

C. GA-004-004 Duty to Report

D. GA-004-005 Accounting of Disclosures

X. **Regulation/Standards**

A. 45 CFR §§ 164.400-414

B. 501.171, F.S.

C. Fair Credit Reporting Act, 15 U.S.C. § 1681a(p)

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Final Approver	Brian Kozik: SVP, COMPLIANCE & PRIVACY	08/2021
	Lucia Pizano-Urbina: AVP, COMPLIANCE	08/2021