Status **Active** PolicyStat ID **10668947**

Origination	02/2010	Area	HIPAA - Privacy
Last Approved	11/2021	Applicability	USA Health
Effective	11/2021		
Last Revised	11/2021		
Next Review	11/2024		

HIPAA Breach Notification

POLICY STATEMENT:

USA Health is committed to conducting business in compliance with all applicable laws, regulations and USA Health policies. USA Health has adopted this policy to ensure compliance with the Health Information Technology for Economic and Clinical Health Act ("HITECH") Breach Notification regulations as modified by the final Omnibus rules which cover improper disclosures to third parties and unauthorized accesses by employees. These regulations require that notification be made to affected individuals and the Secretary of Health and Human Services ("HHS"). In case of a security or privacy breach involving more than 500 individuals, the media must also be notified. Notification is required when the privacy of unsecured patient protected health information has been breached.

POLICY STANDARD:

USA Health shall provide written notification to individuals whose unsecured PHI has been breached as required by law.

PROCEDURE:

1. What Constitutes Unsecured PHI.

A. Definition. "Unsecured PHI" means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individual through the use of a technology or methodology identified by the Secretary of HHS. Unsecured PHI may be written, oral or electronic PHI.

B. Exceptions. PHI which has been encrypted, destroyed or de-identified in accordance with the following standards is not considered Unsecured PHI and therefore is not subject to this policy:

i. Encrypted PHI - Electronic PHI has been encrypted as specified in the HIPAA Security

Rule by "the use of algorithmic process to transform the data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

a. Data at Rest - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111:

b. Data in Motion - Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52.

ii. Destroyed PHI. PHI which has been destroyed, through the destruction of the media on which it is stored or recorded. This shall require:

a. Paper, film or other hard copy media to be shredded or destroyed such that the PHI cannot be read or reconstructed; and

b. Electronic media to be cleared, purged, or destroyed consistent with NIST media sanitation standards, so that the PHI cannot be retrieved.

2. What Constitutes a Breach.

A. Definition. "Breach" means the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of PHI.

B. Exceptions. The following events do not constitute a Breach and therefore are not subject to this policy ("Breach Exceptions").

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of our organization or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rules.

ii. Any inadvertent disclosure by a person who is authorized to access PHI within our organization or our Business Associate to another person authorized to access PHI without our organization or our Business Associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rules.

iii. A disclosure of PHI where we or one of our Business Associates has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

C. Breach Presumed. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rules is presumed to be a Breach unless we or our Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI Involved, including the types of identifiers and the likelihood of reidentification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

D. When Breach is Deemed Discovered. We shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of our organization.

3. Reporting Suspected Breaches; Investigation.

A. All Workforce members and other persons acting under our authority must immediately report any suspected Breach to the USA Health Office of HIPAA Compliance and the Information Technology department.

B. The Office of HIPAA Compliance shall be responsible for investigating the facts and circumstances of a suspected Breach, and for determining whether a reportable Breach has, in fact, occurred. The USA Health HIPAA Breach Decision Tool may be used for such purpose. At the conclusion of the investigation, the Office of HIPAA Compliance will be responsible for documenting the investigation's outcome, including whether the reasons as to why a Breach notification is or is not determined to be necessary.

4. Notification Process.

A. Individual Notification. Following the discovery of a Breach, USA Health shall notify each individual whose Unsecured PHI has been or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of such Breach ("Individual Notification").

i. Timing. Except in cases of a Law Enforcement Delay, an Individual Notification shall be provided without unreasonable delay, and in no case later than sixty (60) calendar days after the discovery of a Breach.

ii. Content of Individual Notification. Each Individual Notification shall be in plain language and shall include, to the extent possible the following information:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

b. A description of the types of Unsecured PHI that were involved in the Breach, such as whether full name, Social Security Number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved. However, this description should not include the actual PHI that was Breached and/or include any sensitive information;

c. Any steps the affected individual should take to protect himself/herself from potential harm resulting from the Breach;

d. A brief description of what we are doing to investigate the Breach, to mitigate the harm to the individual, and to protect against any further Breaches; and

e. Contact procedures for the individual to ask questions or learn additional information about the Breach, which shall include a toll-free telephone number, an E-mail address, website or postal address.

iii. Methods of Delivery for Individual Notification.

a. Written Notice: Sufficient Contact Information. Individual Notification shall be in written form, by first class mail, to the individual at the last known address of the individual, or by E-mail if the individual has agreed to receive such notices electronically. The notification may be provided in one or more mailings as information becomes available. As appropriate and permitted by the Privacy Rules, Individual Notification may be sent to an individual's authorized personal representative.

b. Substitute Notice: Insufficient Contact Information. In the case where there is insufficient, or out-of-date contact information that precludes providing an Individual Notification in writing, a substitute form of Individual Notification reasonably calculated to reach the individual should be provided.

i. Fewer than 10 Individuals. In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) individuals, then such substitute notices may be provided by an alternative form of written notice, telephone or other means. For example, if it is determined that one or more individuals' mailing addresses are out-of-date, but we have current telephone numbers for the individuals in our files, then the individuals may be contacted by phone.

ii. 10 or More Individuals. In the case in which there is insufficient or out-of-date contact information for ten (10) or more individuals, then such substitute notices shall be in the form of either conspicuous posting for a period of ninety (90) days on our home Web site, or a conspicuous notices in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside. Such a Web or media posting shall include a toll-free telephone number that remains active for at least 90 days where individuals can learn whether their Unsecured PHI may be included in the Breach.

c. Urgent Situations. In any case deemed by us to require urgency because of possible imminent misuse of Unsecured PHI, we may provide information to the affected individual(s) by telephone or other means, as appropriate. However, this initial contact shall be followed by written Individual Notification to the affected individual(s).

B. Media Notices. In the event we experience a Breach affecting more than 500 individual residents of a State or jurisdiction, we shall provide notices (*e.g.* a press release) to prominent media outlets serving the State or jurisdiction ("Media Notice"). Except in cases of a Law Enforcement Delay, the Media Notice shall be provided without unreasonable delay, and in no case later than sixty (60) days following the discovery of a Breach and will include the same

information required for an Individual Notification. This Media Notice obligation is in addition to the Individual Notice obligations.

C. Notice to Secretary of HHS. In addition to notifying affected individuals and the media of a Breach, we shall notify the Secretary of HHS of a Breach as follows:

   i. Breaches Affecting More than 500 Individuals. In the event a Breach affects 500 or more individuals, we shall, except in cases of a Law Enforcement Delay, provide the notification contemporaneously with the Individual Notification in the manner specified on the HHS website.

   ii. Breaches Affecting Less than 500 Individuals. For Breaches involving less than 500 individuals, we shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, provide the notification of such Breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.

D. Law Enforcement Delay. HIPAA required Notification may be delayed if a law enforcement official states to us that notification, notice, or posting would impede a criminal investigation or cause damage to national security ("Law Enforcement Delay").

   i. If the statement is in writing and specifies the time for which a delay is required, we may delay such notification, notice, or posting, for the time period specified by the office.

   ii. If the statement is made orally, we shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than thirty (30) days from the date of the oral statement, unless a written statement meeting the requirements in Section 4(d)(1) above is submitted by the official during that time.

E. Notification Documentation. The Privacy Officer shall be responsible for maintaining and retaining copies of any Breach notification to individuals, the media, and Secretary of HHS as well as any Law Enforcement Delay statements. Such documentation shall be maintained and retained in accordance with our HIPAA Compliance plan documentation requirements and standards.

5. HIPAA Business Associates.

Our HIPAA Business Associates shall notify us in the event they discover or suspect any Breach. A Breach shall be treated as discovered by a Business Associate as of the first day on which such Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Business Associate. Such notifications shall be made in accordance with the terms of the HIPAA Business Associate Agreement between the parties and/or as otherwise directed by us.

6. Mitigation: Administrative Obligations.

A. Mitigation. USA Health shall take prompt corrective action to mitigate and cure, if feasible, any harmful effect that is known to us resulting from a breach of Unsecured PHI.

B. Training and Education; Sanctions. Training and education on this policy shall be provided to workforce members and associates as appropriate and necessary for such individuals to carry out their respective duties and responsibilities to our organization. Failure to comply with this policy can result in disciplinary action, including possible termination.

C. Complaints. The Privacy Officer shall be responsible for implementing a process and procedure for addressing complaints concerning the handling of a Breach.

D. Review. All Breaches will be reviewed by USA Health's Office of HIPAA Compliance. All Breaches shall be reported to the University of South Alabama HIPAA Compliance Committee on an annual basis.

7. State Law.

Applicable state law may impose certain breach notification requirements that are more stringent than HIPAA (*e.g.* shorter notification period, notice to additional parties, etc.). To the extent state law is more stringent than HIPAA, state law must also be complied with.

Original Policy No: HIPAA 024

Attachments

HIPAA Security - Cyber-incident Reporting Tool.pdf

USA HIPAA Breach Decision Tool-07.2021_rev2.0.pdf

USA HIPAA Security Incident_rev2.0.pdf

Approval Signatures

Step Description	Approver	Date
	William Grete: Chief Legal Counsel	11/2021
Director, HIPAA	Linda Hudson: Chief HIPAA Compliance Officer	11/2021

Applicability

USA Health, USA Health Children's & Women's Hospital, USA Health Mitchell Cancer Institute, USA Health Physician Enterprise, USA Health Providence, USA Health University Hospital