LifeBridge Health HIPAA Policy 5.
Breach Notification

POLICY

It is the policy of LifeBridge Health or its subsidiaries/affiliates ("Health System") that if there is a breach of unsecured protected health information, then in addition to complying with the Health System's mitigation policy, timely and appropriate notice will be provided to affected patients, the Department of Health and Human Services and the media to the extent required by the applicable HIPAA regulations and this policy.

PROCEDURE

1. A breach notification is required when a breach of unsecured PHI has occurred. Unsecured PHI is PHI that is not encrypted or has not been otherwise physically destroyed (by shredding, burning etc.). A breach is defined as the impermissible acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is *presumed* to be a breach unless the Privacy Officer or designee demonstrates that there is a low probability that the PHI has been compromised. The following four factors must be considered in determining the probability that the PHI has been compromised:

    1.1 The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
    1.2 The unauthorized person who used the PHI or to whom the disclosure was made;
    1.3 Whether the PHI was actually acquired or viewed; and
    1.4 The extent to which the risk to the PHI has been mitigated.

2. A breach of PHI shall be "discovered" on the first day the breach is known (including breaches by a Business Associate) by any person, other than the person committing the breach, that is an employee, officer or agent of the Health System and knows or reasonably should have known of the breach.

3. A breach shall not be deemed to have occurred if:

    3.1 The acquisition, access, or use of PHI was unintentional, was made by an employee or individual acting under the authority of Health System or Business Associate, was made in good faith and within the scope of authority, and does not result in further use or disclosure in an unauthorized manner;
    3.2 The disclosure was inadvertent, was made by a person authorized to access the PHI at the Health System or Business Associate, was made to another person authorized to access PHI at the same Health System or Business Associate or organized health care arrangement in which the Health System participates, and does not result in further use or disclosure in an unauthorized manner; or

3.3 The disclosure of PHI was made to an unauthorized person who would not reasonably have been able to retain such information.

4. If a breach has occurred, an investigation shall be conducted to determine what information has been breached, when the breach occurred, and how many individuals have been affected.

5. If breach notification is required, a notice to the individual(s), Department of Health and Human Services (HHS), and the media, as applicable, shall be made no later than 60 calendar days after the discovery of the breach by the Privacy Officer or designee or Business Associate.

6. If a law enforcement official states that a notification would impede a criminal investigation the organization shall:

   6.1 Delay notification as specified by the official in writing, or;

   6.2 If the statement is made orally, document the statement and delay notification no longer than 30 days from the date of the oral statement, unless a written statement is delivered during that time.

7. The notice to the individual(s) must contain the following information:

   7.1 Brief description of what happened, including the date of the breach and the date of the discovery of the breach;

   7.2 A description of the type of unsecured information involved in the breach (Social Security number, name, address, patient ID number etc.);

   7.3 Any steps the individual should take to protect themselves from the breach;

   7.4 A description of what is being done to investigate the breach and mitigate any damage;

   7.5 Contact information for the Privacy Officer or designee so that patients may receive further information.

8. Notice to individuals shall be provided by first class mail to the individual at their last known address, or if agreement has been given by the individual, by e-mail. Additional information should be provided as it becomes available. If the individual is deceased, information should be provided to the next-of-kin, if known. If contact information for the individual is available and the individual and the Health System have previously agreed, the Health System may notify the individual via telephone or verbally. The Health System must document the conversation. The verbal or telephonic notice must not simply be for the administrative convenience of the Health System.

9. If there is insufficient or out-of-date contact information that prevents proper notice by first class mail, substitute notice may be provided as follows:

   9.1 If there are less than 10 individuals, notice may be provided by alternate means (telephone, e-mail etc.);

9.2 If there are 10 or more individuals, substitute notice shall be in the form of a conspicuous posting on the home page of the Covered Entity or Business Associate's website for a period of 90 days, or a conspicuous notice in major print or broadcast media in the Health System's or Business Associate's geographic area. This notice shall include a toll free number where the individual can learn more information;

9.3 If notification requires urgency because of possible imminent misuse of PHI, notification may be provide by telephone or other appropriate means.

10. Notice shall be provided to the media when the breach of unsecured PHI affects more than 500 patients. Notice shall be provided in the form of a press release.

11. Notice shall be provided to the Secretary of the Department of Health and Human Services through the use of a form posted at www.hhs.gov, or by letter to the Secretary notifying the Secretary of the breach.

11.1 For breaches affecting 500 or more individuals, the organization shall notify the Secretary within 60 days as instructed at www.hhs.gov;

11.2 For breaches involving less than 500 individuals, the Health System or Business Associate shall maintain a log and submit this log annually to the Secretary, no later than 60 days following the end of each calendar year in which the breach was discovered. Instructions for submitting the log are provided at www.hhs.gov .

12. However, regardless of the number of individuals affected, a log shall be kept documenting all breaches of unsecured PHI.

13. A Business Associate shall notify the Health System Privacy Officer or designee of any breach immediately and in any event prior to the deadline for notification of individuals which is 60 days after the discovery of the breach. Such notice shall include all information needed to assess and monitor the breach. The Health System shall notify all affected individuals unless the Business Associate previously agreed to provide notification in case of a breach. However, the Health System is still responsible for such notification and must still document such notification.

14. The Health System shall train all employees and other agents on the policies and procedures concerning breach notification, including how to identify a breach.

15. The Health System must provide a mechanism for individuals to file complaints regarding a breach or other confidentiality issues.

16. The Health System shall have in place appropriate sanctions for employees and agents who fail to comply with the Privacy and Security Standards, consistent with LifeBridge Health HIPAA Policy 1 and Human Resources Policy on Corrective Action/.

17. The Health System may not intimidate or retaliate in any way against any individual who exercises their rights under HIPAA. The Health System cannot compel any individual to waive their privacy rights.

REFERENCES

45 C.F.R. § 164.402
45 C.F.R. § 164.404
45 C.F.R. § 164.406
45 C.F.R. § 164.408
45 C.F.R. § 164.410

Developed 9/1/13

Reviewed 11/13/16