Managing Security Breaches

Member Meeting, January 27, 2023

Gwen Simons, Esq, PT, OCS, FAAOMPT
Simons & Associates Law, P.A.
gwen@simonsassociateslaw.com
Office phone: 207-883-7225
Cell phone: 207-205-2045

1

What is a Security Breach?

- The
  - acquisition
  - access
  - use, or
  - disclosure

of (*unsecured)* Protected Health Information (PHI) in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2

Unsecured v. Secured PHI

- Unsecured PHI has not been rendered unusable, unreadable, or indecipherable to unauthorized persons
- Secured information *has* been rendered unusable, unreadable, or indecipherable – usually through encryption (with regard to electronic PHI) or destruction of the PHI so that it cannot be reassembled or recovered (cross-shredding of paper, proper destruction of hard drives, etc…)
- For guidance on proper destruction of PHI, see https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

3

Breach examples . . . .

- Misdirected Fax
- Sending a group e-mail without using the blind copy box
- Workforce member accesses a medical record for someone they are not treating
- Stolen laptop, UBD drive or other electronic data storage device
- Unauthorized access to your network
- Unauthorized access to data on the back end of your website
- Unauthorized access by cleaning service to PHI left out in your office
- Cyber-attack
- PHI not secured by EMR vendor – accessible to people or companies who are not authorized to access it.

4

"Breach" *excludes*

- unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates.
  - In both above cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

5

Breach presumption . . . .

- An impermissible use or disclosure of protected health information is presumed to be a breach *unless* the covered entity (CE) or business associate (BA), as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment.

6

Risk Assessment Factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

7

Breach Notification Requirements

- Generally, the CE (not the BA, even if the BA is the source of the breach) is the entity required to notify the individuals whose data was breached.
- Notice form:
  - Written by first class mail or email *if the individual has agreed to receive such notices electronically.*
  - *If* your contact information is insufficient or out-of-date
    - For 10 or more individuals, you must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. You must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
    - For less than 10 individuals, substitute notice may be an alternative form of written notice, by telephone, or other means.

8

Time limit for notice

- 60 days to individual unless a law enforcement exception applies
  - This is from the date of the breach, *not* the date the BA notifies you. Therefore, time is of the essence!
  - In your BA Agreements with vendors – make sure the BA has to notify you in 30 days or less so you can meet your 60-day notification. Your BAA can also require the BA to make notification if they are the source of the breach.

9

Requirements for Content of Notice

- a brief description of the breach
- a description of the types of information that were involved in the breach
- the steps affected individuals should take to protect themselves from potential harm
- a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches
- contact information for the covered entity (or business associate, as applicable).

10

Media Notice required for >500 individuals

- When the breach affects more than 500 individuals in a state or jurisdiction . . . .
- Notice to prominent media outlets serving the State or jurisdiction, in the form of a press release.
- Must include the same information as in the written notices to individuals

11

Notice to Secretary of HHS

- Each breach must be reported to the Secretary of HHS by filling out and electronically submitting a breach report form.
- If breach involves >500 individuals, HHS report must be filed within 60 days of the breach.
- If breach involves <50 individuals, the report can be filed on an annual basis, within 60 days of the end of the calendar year (before March 1).

12

Breach Documentation Required

- Maintain documentation that all required notifications were made, or,
- If you determine through your risk assessment that notification is not required because
  - there is a low probability that the PHI has been compromised by the impermissible use or disclosure; or
  - the application of any other exceptions to the definition of "breach"

You need to keep records of your risk assessment.

13

13

Other requirements:

- You must have policies and procedures for how to handle a breach
- You must educate your workforce members (employees *and* independent contractors) on how to recognize a breach and report it.

14

14

Template Policy

- Will be posted later today on the Template Forms, Guides and Policies page of my website - https://simonsassociateslaw.com/need-a-form-for-your-practice-2/

15

15

Questions?

17

17