Oh No! Breach by a Business Associate

Mark Joseph Fox
Privacy & Research Compliance Officer,
American College of Cardiology
Washington, DC

Thora Johnson
Partner & Chair of Healthcare
Practice, Venable, LLP
Baltimore, MD

AMERICAN COLLEGE of CARDIOLOGY

1

Reporting use and disclosure of PHI not contemplated by the BAA

- Report to the Covered Entity any use or disclosure of information not provided for by contract of which it becomes aware, including breaches of unsecured PHI.
- No regulatory deadline unless constitutes a breach.
- BEWARE—there may be a timeframe outlined in the BAA.

AMERICAN COLLEGE of CARDIOLOGY

2

Definition of a Security Incident

- The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the system operations in an information system.
- Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, data, applications, communications, and people.
- No regulatory deadline unless constitutes a breach.
- BEWARE— a timeframe may be outlined by the BAA.

AMERICAN COLLEGE of CARDIOLOGY

3

Definition of a Breach

- Means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI.
- Important exceptions
  - Unintentional by a workforce member and in good faith and within scope of authority;
  - Inadvertent disclosure by an authorized person to a person authorized to access PHI; and
  - Good faith belief that no ability to retain the information.
- Without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
- BEWARE (again)—shorter timeframe may be outlined in the BAA.

AMERICAN COLLEGE of CARDIOLOGY

4

Four Factor Assessment

- An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or 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:
  - Nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - Unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - Extent to which risk to the PHI has been mitigated.

AMERICAN COLLEGE of CARDIOLOGY

5

What does the BAA say?

- What are the requirements for notice to the Covered Entity?
- Do the notice timeframes align with state breach notification laws?
- Who is responsible for completing the Four Factor Assessment?

AMERICAN COLLEGE of CARDIOLOGY

6

What does the BAA say?

- Who is responsible for notifying:
  - Individuals
  - Media (which press, which media)
    - 500 applies at covered entity level
  - Office of Civil Rights
  - State Attorney Generals
  - Other State Notifications (e.g., Departments of Insurance)
  - SEC notifications

AMERICAN COLLEGE of CARDIOLOGY

7

Be Prepared

- Who are the Covered Entities?
- Who is the Privacy Officer at each Covered Entity?
- What does the Business Associate Agreement say about delivery of notice?
- Who is on your breach response team?

AMERICAN COLLEGE of CARDIOLOGY

8

Lessons Learned

- Keep a running list of Covered Entities.
- Periodically update Covered Entity Privacy Officer information.
- There will be variability in risk posture at Covered Entities.
- Be prepared to send supplemental notices as more information becomes available.
- Forensic report sharing.

AMERICAN COLLEGE of CARDIOLOGY

9

Lessons Learned

- Develop Frequently Asked Questions document.
- Which parties are identified in notices?
- Who files on the OCR breach portal?
- Be prepared for media contact.
- Be prepared for your breach to be discussed in privacy and security discussion groups.

AMERICAN COLLEGE of CARDIOLOGY

10

Lessons Learned

- Ensure your breach response team is available for months after the initial notice.
- Be prepared for a document request from the Office for Civil Rights.
- Document, document, document.
- Consistent story across constituents.

AMERICAN COLLEGE of CARDIOLOGY

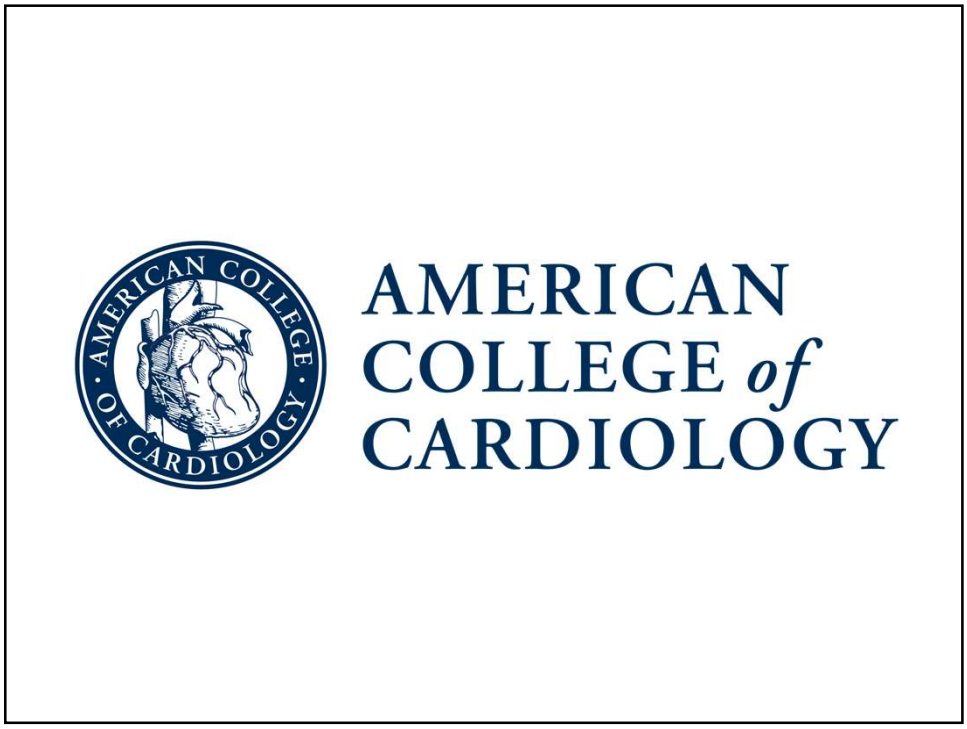
11

Lessons Learned

- Have an established relationship with our Cyber-Liability Insurance provider.
- Revisit your Breach/Incident Response Plan and Privacy Program to incorporate lessons learned from each response.
- Be prepared to receive an influx of due diligence requests from Covered Entities.
- Don't underestimate the stress placed on the organization.

AMERICAN COLLEGE of CARDIOLOGY

12


AMERICAN COLLEGE OF CARDIOLOGY
AMERICAN
COLLEGE of
CARDIOLOGY

13