HIPAA Data Breaches: Managing Them Internally and in Response to Civil/Criminal Investigations

Health Care Litigation Webinar Series

March 22, 2012

Spence Pryor

Paula Stannard

Jason Popp

ALSTON+BIRD LLP

HIPAA/HITECH Act Breach Notification Rule

- Requires notification of individuals, OCR, and, in some circumstances, the media concerning "breaches" involving "unsecured PHI."
- Safe harbor if security measures meet HHS Guidance Standards.
  - Guidance initially issued on April 17, 2009. Posted on HHS's website and updated annually.
- Guidance:
  - Data at rest: Encryption consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
  - Data in motion: Encryption processes that are Federal Information Processing Standards (FIPS) 140-2 validated.
  - Destroy media on which PHI is stored or recorded:
    - Paper, film, or other hard copy media have been shredded or destroyed.
    - Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization.

HIPAA/HITECH Act Breach Notification Rule

- "Breach" is an "unauthorized" acquisition, access, use, or disclosure of [unsecured] PHI that "compromises the security or privacy of the PHI."
- HHS deems "unauthorized" to mean "an impermissible use or disclosure of PHI under the HIPAA Privacy Rule."
  - Not every security incident or violation of the Security Rule constitutes a violation of the Privacy Rule.
- A breach does not include:
  - Unintentional access of PHI by an employee of a covered entity or business associate if
    - The access occurred in good faith, within the scope of employment, and
    - The PHI is not further accessed, used, or disclosed.
  - Inadvertent disclosure by an authorized person within a facility operated by a covered entity or business associate, if no further use or disclosure.
  - Disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized person to whom it was disclosed would not reasonably have been able to retain it.

HIPAA/HITECH Act Breach Notification Rule

- An event "compromises the security or privacy of the PHI" if it "poses a significant risk of financial, reputational or other harm to the individual."
- This requires the covered entity or business associate to do a "risk assessment" to determine if a "breach" has occurred.
  - Disclosure to a covered entity may be low risk.
  - Use or disclosure of PHI in the form of a Limited Data Set (as long as it does not include date of birth and zip code) does not pose a significant risk.
  - Mitigation action can reduce risk.
  - Type and quantity of PHI can be considered.
- If covered entity or business associate determines that event does not pose significant risk, there is no obligation to notify under the Rule.

HIPAA/HITECH Act Breach Notification Rule

Business Associate Obligations:

- Must give notice to covered entity within 60 calendar days of discovery of breach by business associate personnel.
- Must identify each individual whose PHI has been compromised.
- Must provide other information to covered entity to assist in notification of individuals, if such information is available:
  - Description of event.
  - Date of breach.
  - Types of PHI involved.
  - Mitigation actions.

HIPAA/HITECH Act Breach Notification Rule

Covered Entity Obligations

- Within 60 calendar days of discovery of breach, a covered entity must notify the affected individuals by first class mail or email.
  - Business Associate Breach:
    - If business associate acts as an agent to the covered entity, the business associate's discovery will be imputed to the covered entity. Covered entity's 60 days runs at the same time as the business associate's 60 days.
    - If business associate is an independent contractor of the covered entity, the covered entity must provide notification based on when business associate notifies it of the breach.
- If the breach affects more than 500 individuals in the same state or jurisdiction, the covered entity must provide notice to media outlets in the state or jurisdiction.

HIPAA/HITECH Act Breach Notification Rule

Covered Entity Obligations (continued)

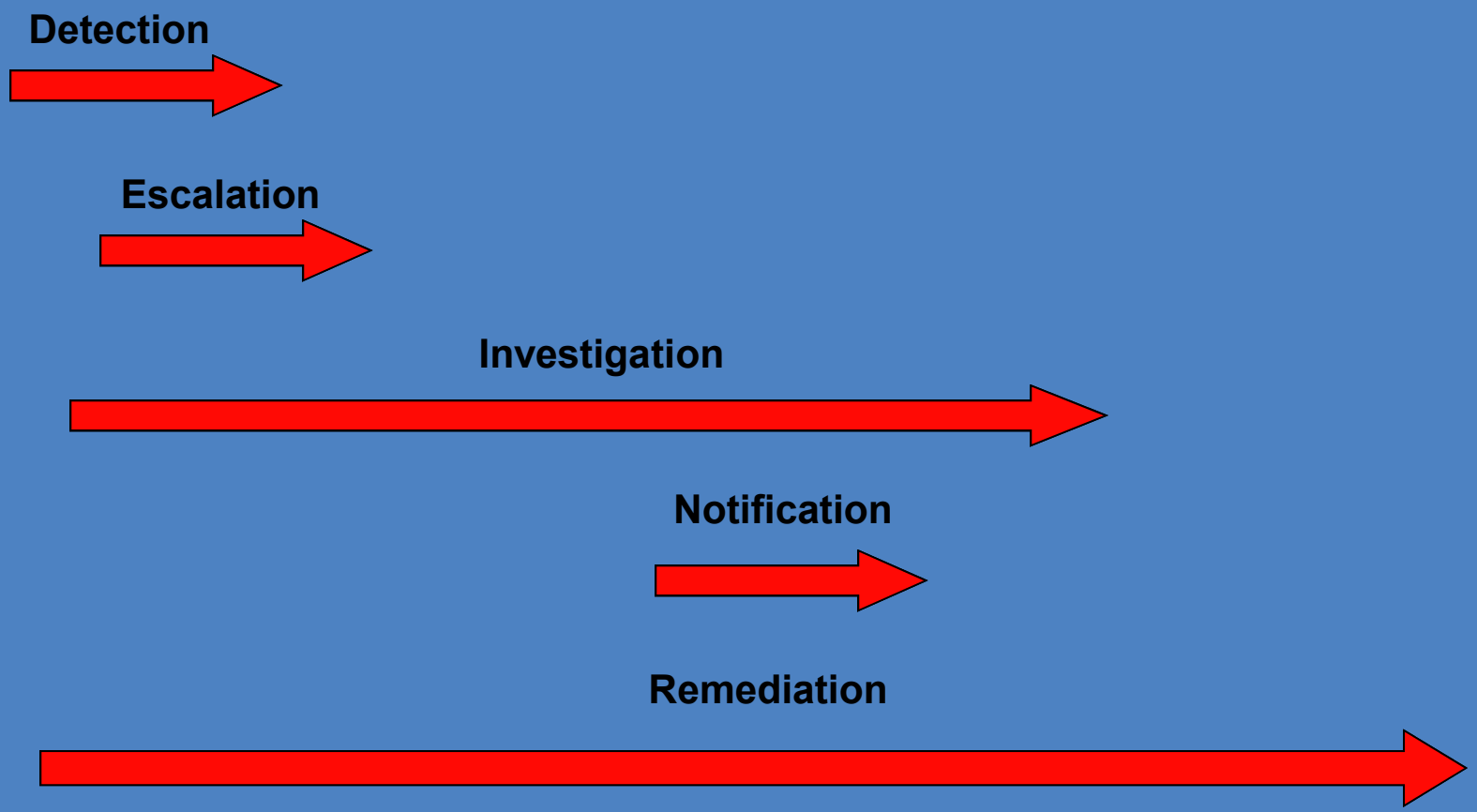
- Notice to HHS/OCR:
  - If fewer than 500 individuals affected by the breach, maintain a record of the breach in a breach log and provide notification to HHS/OCR within 60 days after the end of the calendar year.
  - If 500 or more individuals affected by the breach, provide notice to HHS/OCR at same time as notice to the individuals.
- Notification can be delayed if notification would, in the judgment of law enforcement officials, impede a criminal investigation or damage national security.

HIPAA/HITECH Act Breach Notification Rule

Covered Entity Obligations (continued)

- Content of Notice:
  - Brief description of breach, including date of breach and date of discovery.
  - Types of PHI involved.
  - Steps individuals can take to protect themselves.
  - Actions by the covered entity (or its business associate) to investigation the breach, mitigate the potential harm to the individuals, and to protect against any further breaches.
  - Contact information for individuals to ask questions or obtain additional information, including a toll-free phone number, an email address, website, or postal address

Breach Management Process/Stages



Breach/Incident Response Plan

- Designate Incident Response Team and Team Leader. Maintain 24-hour contact information for members and alternates.
  - Compliance Officer
  - Privacy Officer
  - Security
  - Information Security
  - Legal
  - PR/Communications
  - Human Resources
  - Customer Service/Patient Relations
  - Business Units
  - Outside Consultants?

Breach/Incident Response Plan (continued)

- Establish an internal notification/reporting process.
- Checklists of steps to be taken or considered.
- Plan to document all actions considered and/or taken and reasons for decisions.
- Regulatory and law enforcement agencies that need to be contacted.
- Plan for post-response review, risk remediation, and process improvement.

Breach/Incident Response Checklist

- Form or activate Internal Response Team to coordinate management of and response to the incident.
- Perform investigation.
- Secure third party forensic investigation support (if necessary).
- Develop detailed chronological investigation report/incident report.
- Develop Public Relations/Communications Strategy.
- Assess NYSE/Nasdaq, SEC disclosure requirements.
- Establish call center resources.
- Notification standards, sequencing, delivery, and response.
- Post-response review, risk remediation and process improvement plan.

Is the incident a HIPAA/HITECH Act Breach?

- Does the incident involve an acquisition, access, use, or disclosure of PHI that would not be permitted under the Privacy Rule?
- Is the PHI unencrypted or unsecured?
- Does the incident fall into one of the exceptions?
  - Unintentional access of PHI by an employee of a covered entity or business associate if
    - The access occurred in good faith, within the scope of employment, and
    - The PHI is not further accessed, used, or disclosed.
  - Inadvertent disclosure by an authorized person within a facility operated by a covered entity or business associate, if no further use or disclosure.
  - Disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized person to whom it was disclosed would not reasonably have been able to retain it.
  - Disclosure involved Limited Data Set (without date of birth and zip code).

Is the incident a HIPAA/HITECH Act Breach?

- Does the risk assessment indicate that the incident "poses a significant risk of financial, reputational or other harm to the individual"?
  - Was the disclosure to another covered entity?
  - Did the recipient return the PHI and agree not to use it or further disclose it?
  - How specific and sensitive is the PHI? Is it only the association of an individual's with a comprehensive health plan or large general hospital (with no indication of type of treatment or health condition)?
- Only if the incident poses a significant risk of financial, reputational or other harm to the individual does the incident constitute a "breach" under the HIPAA/HITECH Act Breach Notification Rule that requires notifications.

Consider Other Breach Notification Laws

- Most States have breach notification laws, with the potential for different notice requirements, different standards for when notice is required, and different timelines for notice.
  - State law requirements are unlikely to be preempted by HIPAA/HITECH Act requirements.
  - The covered entity/business associate needs to consider the applicability of the laws of the State where
    - The breach occurred.
    - The affected individuals reside.
- The FTC breach notification rule
  - Is similar.
  - Governs information breaches by personal health records vendors, related entities, and their service providers.

OCR Investigations

- OCR's Means of Initiating Review of Covered Entity/Business Associate
  - Complaint.
  - Breach Notification.
  - Compliance Review.
  - Privacy and Security audit program.
- Covered entities/business associates required to cooperate, respond to OCR, and provide relevant documents and information.
- Current Enforcement Rule requires OCR to seek informal resolution of complaints and investigations.

OCR Investigative Requests

- OCR investigative letters
  - Tend to reference or specifically quote the entity's breach notification to OCR.
  - Identify provisions of the Security, Breach Notification, and Privacy Rule that could be violated as a result of the breach identified in the breach notification.
  - Usually do not provide any further detail on the alleged violation(s).
  - Require the entity to respond to specific data requests, but permit the entity to submit additional data as it desires.
  - Generally provide 21 days for the entity to respond.

Responding to OCR Investigative Requests

- Collect and provide all requested documents, as well as such documents as may demonstrate the entity's compliance with the HIPAA Privacy, Security, and Breach Notification Rule.
- In the responses to the information and document requests, provide explanatory commentary to describe the documents provided in the context of the entity's compliance with the requirements of the Rules.
- Provide an overview in which to explain the incident and to discuss compliance with the Rules in general and with the provisions of the Rules alleged to be potentially violated in particular.

Defending Against Criminal HIPAA Investigations

- Assess the allegations if they are made available
- Collect and review documents ASAP
- Attempt to limit your initial document production until government has a better understanding of how your program/policies comply with HIPAA
- Produce requested documents with explanations
- Explain to government how program/policies comply with HIPAA

Critically Assess the Allegations

- If investigation begins with a letter containing the allegations, then frame defense accordingly
- If investigation beings with simple document request, inquire into government's concern
  - If government will not divulge information, read between the lines of the document request
- Frame defense and behavior in line with the allegations

Collect and Review Documents

- Collect all requested documents and any other documents that may assist with defense
  - For example, collect all documents that help demonstrate company's compliance with HIPAA and protection of PHI
- Determine course of defense based off available documents
  - Identify documents and witnesses that support compliance with HIPAA

Produce documents with "Color"

- Provide documents to investigators with descriptions and explanation
  - HIPAA prosecution is a relatively new area, so use document production as opportunity to educate investigators
- Develop themes of privacy and confidentiality in document productions
  - Produce documents that convey how company explains use of PHI to its employees
  - Produce company documents relating to training, compliance, and privacy safeguards

Provide Roadmap to Investigators

- Develop a roadmap that guides investigators to correct conclusion. Show:
  - How relevant policies work
  - Mechanisms used to protect PHI
  - Who has access to relevant PHI, and how that access is appropriately restricted
    - E.g. explain why that access is appropriate under HIPAA
  - How access to PHI is restricted to the minimum that is necessary for administration
  - When and how PHI may be disclosed, and why such disclosure complies with HIPAA

Meet with Investigators

- If beneficial, request opportunity to meet with investigators
  - Walk investigators through company policies and explain how it complies with HIPAA
  - Discuss the potential scenarios that concern investigators and explain why they do not implicate HIPAA concerns
    - E.g. If investigators are concerned with Business Associates' use of PHI, explain why that use is appropriate and allowed under HIPAA
  - Again, use opportunity to educate investigators on HIPAA provisions and why company policies comply

Recent Enforcement Actions and Investigations

- Investigations into employer and Business Associates access of PHI
- Inappropriate physician or nurse disclosure of PHI
  - Inappropriate disclosure to patient's employer
  - Inappropriate disclosures to patient's presumed "agent"
- Investigations into employer safeguards for protecting employee PHI

Questions?

Spence Pryor
(404) 881-7978
spence.pryor@alston.com

Paula Stannard
(202) 239-3626
paula.stannard@alston.com

Jason Popp
(404) 881-4753
jason.popp@ alston.com

ALSTON+BIRD LLP