



Data Privacy and Security Update

Erin Fleming Dunlap
Shareholder, Polsinelli PC

Polsinelli PC. In California, Polsinelli LLP

In the News...



real challenges. real answers. sm

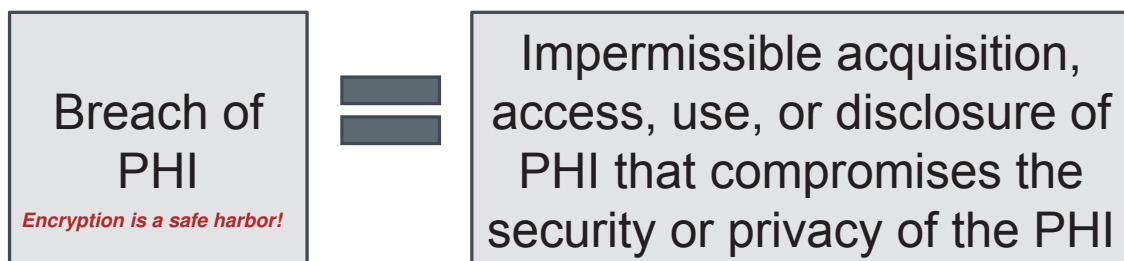
Agenda

- Basics of a Breach
- Recent Settlements/Enforcement Actions
- State Actions On the Rise
- Need for Cyber Liability Insurance
- Status of the HIPAA Audit Program
- Key Takeaways/
Recommendations



real challenges. real answers. sm

Definition of a Breach under HIPAA



Three exceptions:

1. Unintentional acquisition, access or use of protected health information ("PHI") by an individual under Covered Entity ("CE") or Business Associate ("BA") authority that is ***made in good faith*** and ***within the scope of the individual's authority***, and ***does not result in further unauthorized use or disclosure***
2. Inadvertent disclosure by authorized individual to another authorized individual at the same CE or BA that ***does not result in further unauthorized use or disclosure***
3. Disclosure of PHI where CE or BA has ***good faith belief*** that the unauthorized recipient ***would not reasonably have been able to retain the PHI***



real challenges. real answers. sm

Presumption of Breach / Risk Assessment

- If the impermissible acquisition, access, use, or disclosure does not meet one of the exceptions to the definition, it is ***presumed*** to be a breach.
- May overcome the presumption by showing a low probability that the PHI was compromised.
- To assess probability, perform ***written*** risk assessment of the following factors:
 1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 2. The unauthorized person who used the PHI or to whom the disclosure was made;
 3. Whether the PHI was actually acquired or viewed; and
 4. The extent to which the risk of PHI has been mitigated.



real challenges. real answers. sm

Breach Notification Requirements

- CE must notify individuals and Office for Civil Rights (“OCR”)
- BA must notify CE
- Notice must contain:
 - Description of Breach
 - Types of PHI involved
 - Steps the individual should take to protect him/herself
 - Steps the CE took to investigate, mitigate and protect from future breaches
 - Contact information/procedure
- Timing and method of notification depends on number of individuals involved



real challenges. real answers. sm

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

Title search: Data Privacy and Security Update

Also available as part of the eCourse

[Healthcare Compliance and Enforcement](#)

First appeared as part of the conference materials for the
27th Annual Health Law Conference session

"Data Privacy and Security Update"