Managing Breaches: Understanding State and Federal Law

Aimee Wall
UNC School of Government

April 21, 2010

UNC
SCHOOL OF GOVERNMENT

www.sog.unc.edu

Uh oh…

- An employee lost a thumb drive with patient data on it…
- A laptop was stolen…
- An employee accidentally gave Jill a copy of Aimee's health records…
- An frustrated employee "borrowed" some social security numbers from patient records…

What should you do?

Managing a Breach

- Reviewing the legal guideposts
  - Federal: HIPAA/HITECH
  - State: Identity theft law
- Disclaimer:
  - ***Please remember that I am not a security expert or techie. I am merely a lawyer.***
-

What is a breach?

- Federal
  - Acquisition, access, use, or disclosure of PHI
  - In a manner not permitted by the HIPAA Privacy Regulation
  - Which poses a significant risk of financial, reputational, or other harm to the individual

What is a breach?

- State
  - An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data
  - Containing personal information
  - If
    - Illegal use of the personal information has occurred or is reasonably likely to occur *or*
    - Incident creates a material risk of harm to a consumer

What is a breach?

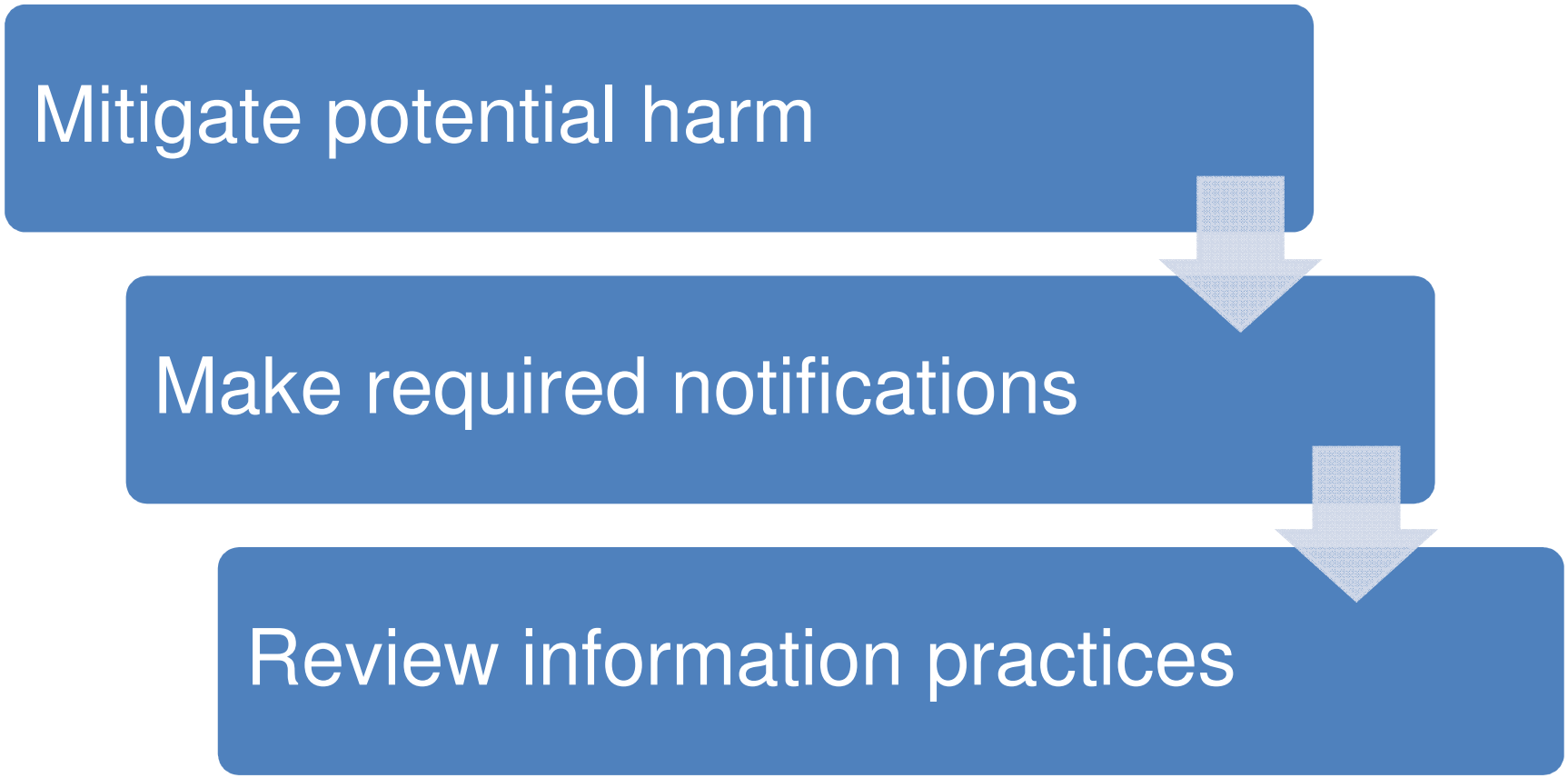
Similarities

- Unauthorized access, use, acquisition or disclosure of information
- Risk of harm required
- Encryption helps!

Differences

- PHI v. Personal Information
- Risk of harm threshold
  - Fed: Significant risk of harm
  - State: Illegal use or material risk of harm

What should you do?



Mitigation

- HIPAA requirement
  - Must mitigate to the extent practicable, any harmful effect that is known to the health department
    - Response will vary depending on the circumstances
    - No guidance regarding what constitutes appropriate mitigation

Notice

Federal	State

• Individual
• Media if >500
• Feds
  – Annual log
  – If >500, without unreasonable delay
	• Individual
	• State if >1,000
	• Consumer reporting agencies if >1,000

Review internal practices

- Accounting
  - Will this be reflected?
- Review policies and procedures
  - Should anything be changed?
- Evaluate workforce members
  - Are sanctions called for?
  - Is re-training necessary?

Consequences

- Enforcement
  - Complaint driven
  - Civil money penalties (higher now!)
  - New authority for states to enforce
- Private right of action?
  - Not recognized under state law or HIPAA but other types of claims may point to these laws as establishing standard of care
    - *See* Acosta v. Byrum, 638 S.E.2d 246 (N.C.App 2006)

QUESTIONS?