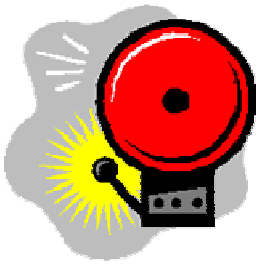
HIPAA Breaches & Employment Issues

Jill Moore, UNC School of Government
April 2015

UNC SCHOOL OF GOVERNMENT www.sog.unc.edu

What is a breach?

- Acquisition, access, use, or disclosure of protected health information (PHI) that:
  - Is not authorized by the HIPAA privacy rule, and
  - Compromises the privacy and security of the PHI.
- Breach is ***presumed*** unless:
  - A specific exception in the rule applies, or
  - A risk assessment shows a low probability that PHI was compromised.



What are the exceptions?

- PHI could not reasonably be retained
- Access is unintentional and by a workforce member or business associate acting in good faith

- Inadvertent disclosure is made to another person within the CE or BA who is authorized to access PHI

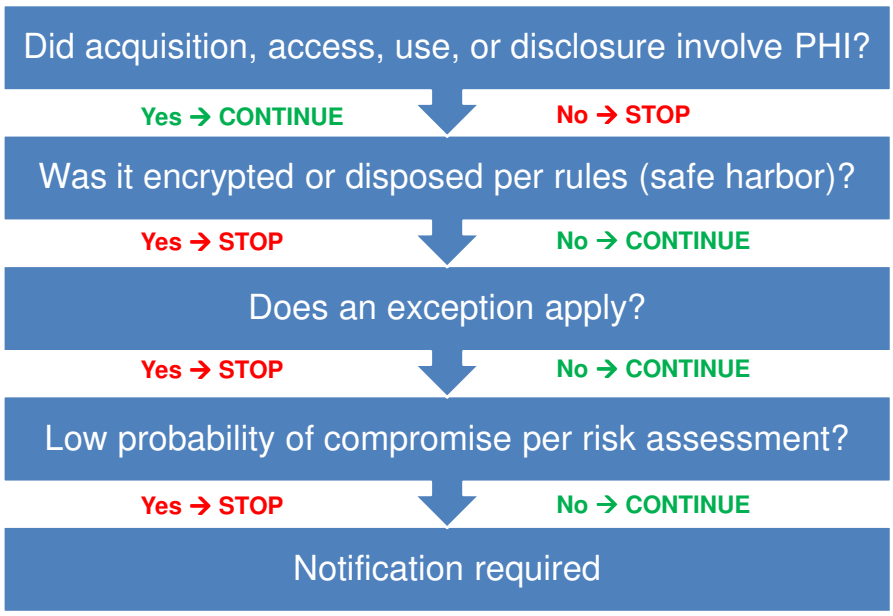
Exception = not a breach (but document it)

Risk Assessment

What it is:	Minimum factors:
• Analysis you undertake to demonstrate low probability that PHI was compromised • Demonstrated low probability of compromise defeats the presumption that unauthorized acquisition, access, use, or disclosure was a breach	• Nature and extent of PHI, including types of identifiers & likelihood of re-identification • Unauthorized person who received disclosure or used PHI • Whether PHI was actually acquired and viewed • Extent to which any risk to PHI has been mitigated

Safe harbor

- Don't have to notify if:
  - PHI was encrypted, or
  - PHI was disposed in keeping with HHS guidance on secure disposal



Notification prep: date check

- If required to notify, must do so "without unreasonable delay" – no later than 60 days after breach discovered
- Breach deemed discovered even if no actual knowledge, if reasonable diligence would have revealed it

Recipients & timing	• Affected individuals – within 60 days
	• US DHHS
	  • ≥ 500 individuals – contemporaneous
	  • < 500 - annual report
	• Media if > 500 – within 60 days.

Content	• Description of incident • PHI involved • Advice to individuals to minimize harm • Actions taken to investigate and mitigate • Contact information for more info
Method	• Written letter (standard) • Email if prior agreement to email notification obtained • Telephone if urgent (also send written)

State Law on Breaches

- Breach: unauthorized access to or acquisition of records or data with "personal information," which means name plus something that could be used to commit ID theft or threaten finances (SSN, DL number, financial account numbers, etc.)
- State law requires breach notification, if:
  - Illegal use of the information has occurred, or
  - Illegal use of the information is reasonably likely to occur, or
  - The incident creates a material risk of harm to a consumer.

What else should you do?

- ✓ **Investigate** the circumstances
- ✓ **Mitigate** harm to individuals
- ✓ **Account** for disclosures (include in accounting log or other mechanism you use to provide accounting to individuals who request it)
- ✓ **Follow-up with employees** – apply sanctions, review training

HIPAA sanctions policy

- Must have and apply appropriate sanctions against workforce members who violate HIPAA or your entity's privacy policies and procedures
  (45 CFR 164.530(e))
- What is your sanctions policy?

Breach resources

- HIPAA regulations: 45 CFR 164, subpart D (sections 164.400 – 164.414)
- US DHHS resources:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/