HIPAA BREACHES

UW Medicine

A BREACH IS:

- Unauthorized acquisition, access, use or disclosure of unsecured* PHI in a manner not permitted by the HIPAA privacy rule (for TPO) that compromises the security and privacy of PHI

  *unsecure PHI is PHI that is not rendered unusable, unreadable, or indecipherable

- "Impermissible use or disclosure of PHI" is presumed to be a breach unless there is a low probability that PHI has been compromised

UPDATED HIPAA

- Replaces the breach notification rule's "harm" threshold with a more objective standard
- Formerly, reportable breach was IF potential harm threshold was reached
- Business Associates now held to same standards

BREACH RISK ASSESSMENT

A breach is presumed to be a breach unless the covered entity (CE) or business associate (BA) demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment of:

- ✓The likelihood of re-identification of the information
- ✓Consider whether the unauthorized person has obligations to protect the privacy and security of the info
- ✓ Was the PHI actually acquired or viewed
- ✓The extent to which the risk to the PHI has been mitigated

BREACH ASSESSMENT TOOL

- Encryption

  If Yes – Not a Breach
- Acquisition, access or use of PHI by a workforce member, in good faith, and without further use or disclosure not permitted by the Privacy Rule

  If Yes – Not a Breach
- Inadvertent disclosure to a person authorized to access PHI, without further use or disclosure permitted by the Privacy Rule

  If Yes – Not a Breach
- Where there is a good faith belief that the unauthorized person would not be able to retain the information

  If yes – Not a Breach

BREACH NOTIFICATION REQUIRED

- Individual patients must be notified within 60 calendar days of discovery date
- Substitute Notice – if 10 or more returned or unknown addresses
- Notice to media – if 500 or greater
- Notice by Business Associates to Covered Entities
- Notice to OCR – if 500 or greater, immediate

Under 500, breaches logged and reported annually

BREACH NOTIFICATION –PATIENT

- Required within 60 calendar days of discovery date
- In written form by first class mail (or email if affected individual has agreed to receive such notices electronically)

Include:

- ✓Brief description of breach
- ✓Description of types of information involved in breach
- ✓The steps the individual should take to protect themselves from potential harm
- ✓A brief description of what the CE is doing to investigate the breach, mitigate the harm and prevent future breaches
- ✓Contact information

SUBSTITUTE NOTICE

If the CE has insufficient or out-of-date contact information for 10 or more individuals, the CE must provide a substitute notice for 90 days by:

- ✓Posting the notice on the home page of CE's website for 90 days **or**
- ✓Providing the notice in major print or broadcast media where the affected individuals likely reside
- ✓Providing a toll free number to learn about the breach

MEDIA NOTICE

- Required when affects greater than 500 residents of a state or jurisdiction
- Likely to be in the form of a press release to appropriate media outlets serving the affected area
- Must be provided without unreasonable delay and in no case later than 60 calendar days
- Must include same information in individual notice

BREACH BY A BUSINESS ASSOCIATE

- The BA must notify the CE following the discovery of the breach – no later than 20 calendar days (per UW's BA)
- BA should provide the CE with the identification of each individual affected plus any other available information
- The CE is ultimately responsible for ensuring individuals are notified
- CE may delegate the responsibility of providing individual notices to the BA
- CE and BA should consider which entity is in the best position to provide notice to the individual

BREACH NOTICE -HHS

- URL:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

- Fill out electronic submission
- If breach 500 affected individuals or greater notify OCR no later than 60 calendar days
- If fewer than 500 – notify OCR no later than 60 calendar days after the end of the calendar year in which the breach was discovered
- OCR will look for an accounting of disclosures

PP 29 NOTIFICATION OF IMPERMISSIBLE USE OR DISCLOSURE OF PHI

- When a CE is notified or discovers a potential breach of PHI, (including a limited data set), the CE must provide written notification to appropriate parties when unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a privacy breach

HSA NOTIFICATION

- Components immediately notify Dave Anderson, HSA Executive Director, of actual or suspected incident
- HSA contacts UW Medicine Compliance as subject matter experts
- HSA follows up with components regarding investigation
- HSA maintains summary of accidental disclosures and resolution
- HSA engages with components in remediation effort