HIPAA BREACHES-LARGE TO SMALL

WHAT TO DO WHEN YOU ARE FACED WITH A BREACH

LORI CUSTER, JD, CHC, RHIT, CCA

WHAT CONSTITUTES A LARGE BREACH?

500 is the magic number!!

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

Make sure you check with your States AG to see what your reporting requirements are from a state level.

What Constitutes a Small Breach? 500 is the magic number!!

- Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.
- Make sure you do not miss your deadlines!

The Risk Assessment Is Your Holy Grail

- Develop an Action Plan. (See handout)
- For every potential breach preform a Risk Assessment (See handout).
- Risk Assessment is your step by step guide to determine if you need to report the breach to an individual, OCR or the media.
- The Risk Assessment can be requested by OCR to help determine a fine.

Large Breaches and Requirements When a Breach Has Been Determined

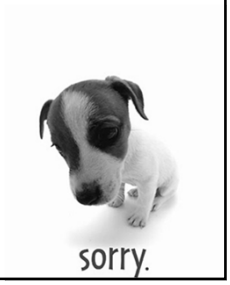
- Covered Entity (CE) is ultimately responsible for the breach notification, however the CE can delegate that responsibility to the Business Associate.
- Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice **to prominent media outlets serving the State or jurisdiction**. Covered entities will likely provide this notification in the form of a press release to **appropriate media outlets serving the affected area (See handout).** Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Large Breaches and Requirements When a Breach Has Been Determined, Cont.

- Post a notice on your website. (See handout)
- The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.

Small Breaches and Requirements When a Breach Has Been Determined

- Contact the patient via USPS within 60 days-(See handout).
- If the patient calls you back for additional details, you must comply.
- Offer the patient a year of credit monitoring- (See handout).
- Apologize, apologize, apologize!



Reporting to OCR

- Report online via https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
- Make sure you ***do not*** miss deadlines to report.
- Report either 60 days from the large breach (500+), or within 60 days from December 31st of the prior year for small breaches.
- Tell a story.
- Make sure you give thorough, complete and up-to-date contact information, especially email address.

What To Do When OCR Comes-a-Calling!

- TAKE A DEEP BREATH!!!
- You will receive an email detailing the information that OCR is requesting.
- You will receive a letter following the email.
- Respond promptly that you have received the information and validate that they have the correct contact information.
- Request a “Read” and “Delivery” receipt to your emails.
- Do not miss deadlines!

It’s A Dance!

- Generally they will request details around the breach.
- Almost always they will be looking for a Security Risk Assessment!
- They will request copies of your Policies and Procedures.
- Response should be organized to respond to the questions. (See handout)

Feel free to contact me:

Lori Custer, JD. CHC
221 Technology Parkway
Rome, GA 30165
762-235-1022
Lori.Custer@harbinclinic.com

QUESTIONS?