DATA BREACHES: HOW TO AVOID THEM AND WHAT TO DO IF IT HAPPENS

Emory IRB Webinar
January 8, 2015

ACKNOWLEDGMENTS

Thanks to Kris West for the information provided for this webinar

DEFINITIONS

Protected Health Information (PHI)

Information about Health, Health Care, Payment for Health Care + Identifiers + Covered Entity **(3 elements)**

Example: Patient diagnosis + MRN + Used by Emory nurse in EUH

Covered Entity = Health Care Provider, Health Care payer, Health Care Clearinghouse

- Covered Entity at Emory: Emory Clinic, all hospitals, SOM, SOPH, SON, psychological counseling centers.

DEFINITIONS

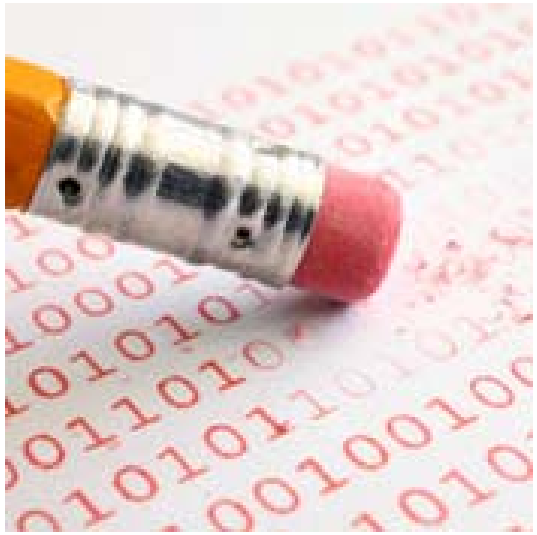
Identifiers

- Names , Dates, Full face image/photo, Phone & Fax #, Address, Health Plan #, SSNs, Certificate/License #, Acct. #, License Plate #, Vehicle ID/Serial #, URL & IP #, Biometric Identifiers, Any other unique identifying item/code.

De-identified health information – data stripped of identifiers – does not constitute PHI.

- Another method of de-identification is to show, using statistical methods, that a data piece cannot be linked with a patients

Remember: Despite appearing de-identified, if you or your team members have the code to identified the data again, the IRB will not actually consider data as de-identified



DEFINITIONS

HIPAA: Privacy Rule – Essentially allows disclosure of PHI only for **T**reatment, **P**ayment or healthcare **O**perations (TPO). Otherwise, there must be an Authorization or Waiver of Authorization (*)

- Key Point: Research is NOT part of TPO

Security Rule – Supplements Privacy Rule (subpart C)

- Applies to electronic PHI (ePHI)
- Goals: Protect **CIA** (**C**onfidentiality, **I**ntegrity, and **A**vailability) of PHI

HIPAA Authorizations are reviewed and granted by the IRB: they should contain certain elements such as information of data to be used or disclosed, purposes, dates of expiration (or events).

(*) The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

WHAT IS A DATA BREACH?

An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

Exceptions to the definition of "breach"

- Unintentional acquisition, access or use of data by a person under the covered entity, made in good faith and within the scope of authority.
- Inadvertent disclosure of PHI by authorized person to another authorized person. Data cannot be used or disclosed in a way not allowed by the Privacy Rule.
- Data disclosed to an unauthorized person but the covered entity has a good faith belief that the person would not be able to retain the information.

(*) From:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

EXAMPLES OF DATA BREACHES (FROM REAL REPORTS RECEIVED BY IRB)

Data entry person took subjects' binders home to finish work later. Took bus to go home and forgot to take them. Binders contained patients' names, dates and diagnoses.

Research staff was entering data at a coffee shop and left they computer at the table to get more coffee. Coming back to the seat, the computer was gone. The computer was not encrypted and the data contained subjects' names, MRN and SSN.

Doctor took medical records home to complete dictations. When shopping at a local grocery store, someone broke into the car and stole the computer and the bag with patient records.

Coordinator sent email to all study participants instead of one, and the email included the date of study visit. The study is on HIV and the email contained the patient names and email addresses.

DATA BREACHES AND UNANTICIPATED PROBLEMS

An Unanticipated Event is an event which meets all of the following:

1. Unanticipated
2. related to study participation, and
3. involving risk to participants or others.

If criteria are met, the event is reportable in 10 business days to the IRB.

So is a data breach an unanticipated problem? Presumptively yes, since it would likely meet all three criteria.

WHAT TO DO IF THIS HAPPENS TO ME?

1. Have an account of what happened, and the data that has been compromised.
2. Contact Office of Research Compliance to report the information to the Privacy Officer (Kris West).
3. Contact the IRB office (if research related), and report it as an event at an Emory facility.
4. If information was sent via email, ask recipient to delete the email, including from the trash folder. Document if recipient saw information, and make sure the data is not kept by unauthorized people.
5. If information was lost (hardcopies), take every step to try to retrieve it. Document your efforts.
6. Determine what went wrong and how can you avoid it in the future.

WHAT ORC DOES WITH THIS INFO?

1. Breach Notification – Required if unauthorized disclosure, use, acquisition, or access compromises the security or privacy of the PHI by posing a significant risk of financial, reputational or other harm to the individual.
   - Timetable for Notice – No later than 60 days following discovery of a breach
2. Privacy Officer determines how breach occurred, who was affected, information affected, steps necessary to mitigate damage and reduce/eliminate risk.
3. Breach analyzed by Emory Breach Notification Team.
   - Team composed of Emory's Chief Information Officer, Security Officer, Privacy Officer for University and EHC, Associate General Counsel, and the Director of Risk Management.

WHAT THE IRB DOES WITH MY REPORT?

Review as a possible UP: First sending to the Compliance Review Team, then to a full board meeting.

IRB will require a plan to fix (if possible) and avoid issue in the future.

After issue is reviewed, IRB may recommend contacting subjects or reconsenting.

If the breach is considered an unanticipated problem, notifications are sent to:

- Department chairs and institutional officials
- FDA (if involving a drug, device or biologic, approved or not)
- OHRP (if funded by federal money)
- Study sponsor or funding agency, if required per contract.

OTHER COMMON HIPAA ISSUES

*(These m*ay not represent UPs or data breaches but may be noncompliance)

- Retrospective chart reviews that did not stay between the IRB approved dates.
  - May require breach notification in some cases.
- Subject did not sign HIPAA document.
  - Remember: cannot use subject's data for research!
- HIPAA form did not contain all required elements.
- HIPAA form had an expired date or event.

HOW TO AVOID BREACHES

Work inside VPN

Do not use personal email to send information for work

If emails are sent outside Emory (e.g. to sponsor), make sure you are not including any PHI with the email

Do not take records home, under any circumstance

Make sure your laptop is encrypted (and other electronic storage devices for that matter!)

Retrospective chart review: collect data for research within the dates approved by IRB.

QUESTIONS?

IRB Contacts on the QA and Education team:

- **Maria G. Davila**
  (404)712-0724 or maria.davila@emory.edu
- **Shara Karlebach**
  (404)712-0727 or shara.karlebach@emory.edu
- **Kevin Wack**
  (404)712-5220 or kwack@emory.edu
- **Sean Kiskel**
  (404)712-0766 or skiskel@emory.edu
- **Heather Smith**
  (404) 712-8689 or heather.smith@emory.edu

THANK YOU!

Please consider taking a moment to complete our survey, link located on the webinars page of the website.