OBER | KALER
Attorneys at Law

Breach, Enforcement, and Beyond:

HIPAA Breach Notification Analysis and OCR Enforcement Activities

September 17, 2014

Your Presenters

Paul W. Kim
pwkim@ober.com

Hannah M. Whitman Clark
hmwclark@ober.com

Welcome

You may download the slides by clicking the PDF link in the upper left corner of your screen.

Also on the left is a **Q&A box** where you may type your questions. We'll look at those questions at the end of the program and answer as many as we can.

At the end of the program, you'll receive an **email with a link to a survey**. Please take a moment to fill that out and give us your feedback.

OCR Enforcement

- Since 2011:
  1) Impermissible Uses & Disclosures
  2) Safeguards
  3) Access
  4) Minimum Necessary
  5) Mitigation

- Impermissible Uses and Disclosures has been the top issue since 2004

Recent Enforcement Actions

- Parkview Health System – medical records dumping, $800,000
- NYP and Columbia University – PHI made publicly available on the internet, lack of policies and protections, $4.8 million
- Concentra – theft of unencrypted laptop, $1.7 million
- QCA Health Plan – theft of unencrypted laptop, $250,000
- Skagit County, WA – PHI made publicly available on a server maintained by the county, $215,000

Lessons Learned

- Complaint Driven
- Second Wave of Audits
- HIPAA Training
- Policies & Procedures
- Standard Operating Procedures
- Security Risk Assessment

Lessons Learned

- Always impose minimum necessary when applicable
- Audit compliance plan to specifically identify potential areas for leaks
- Establish reasonable safeguards
- Act promptly to mitigate

So you think a breach may have occurred….

Breach

- Breach = acquisition, access, use, or disclosure of PHI in a manner not permitted by the regulations *which compromises* its security or privacy
- Regulatory Exceptions:
  1) Unintentional acquisition, access, or use of PHI by a workforce member if made in good faith and within the scope of authority, so long as it does not result in further prohibited use or disclosure
  2) Inadvertent disclosure from one authorized person to another from the same entity where it is not further impermissibly used or disclosed
  3) Disclosure where the entity has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information

If the regulatory exclusions don’t resolve your concern…

LoProCo Risk Assessment

The breach is *presumed* unless, through a risk assessment, the entity determines that there is a LoProCo:

Low

Probability that the data has been

Compromised

LoProCo Factors

4 Primary Factors:

1) Nature and Extent of the PHI;
2) To whom the disclosure was made;
3) Whether the PHI was actually acquired or viewed;
4) Extent of mitigation

** Document, Document, Document **

HYPO 1

A hospital sent a fax containing the medical record number of one patient and the date of service to the wrong physician practice.

Breach?

Need to disclose?

What if recipient physician calls the hospital and says he shredded it.

HYPO 2

Durable Medical Equipment supplier sends 300 invoices with patient names, addresses, names of medical devices, and charge amounts to wrong patients.

Breach?

Need to disclose?

What if the envelope is returned as undeliverable?

Questions?

More questions? Contact us.

Paul W. Kim
pwkim@ober.com

Hannah M. Whitman Clark
hmwclark@ober.com