Health Information Privacy & Security:
Recent Developments & Enforcement Actions

Healthcare Enforcement Compliance Institute
October 29, 2017

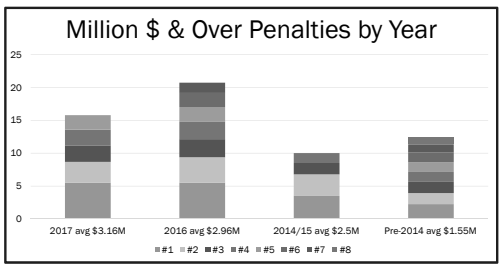
Joan M. Podleski, CHRC, CCEP, CHPC
Chief Privacy Officer,
Children's Health, Dallas

R. Brett Short, CHC, CHPC
Chief Compliance Officer
UK Healthcare, University of Kentucky

AGENDA

- Introductions
- Trends in Large $ Penalties
- Enforcement Themes from Recent and/or Large $ Cases
- Audit Updates
- Questions

23 Penalties over $1,000,000



Focus on Risk Assessments

Think HIPAA's No Big Deal?

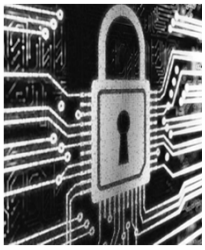
- Failure to address or fully remediate risks identified and documented prior to incidents have resulted in recent fines of **$3.2M** and **$5.5M**
  - *Access controls to ePHI – former employee ID*
  - *Encryption of mobile devices*

Think HIPAA's No Big Deal?

$5.5Million for failure to:

- *Conduct a thorough risk assessment for ALL their ePHI (not just the EMR);*
- *Have sufficient physical controls to data centers;*
- *Obtain assurances from Business Associates on safeguarding ePHI;*
- *Protect an unencrypted laptop.*

Think HIPAA's No Big Deal?



$2.7Million for **failure to:**

- *Perform a full risk assessment for all ePHI;*
- *Store ePHI with a cloud provider without a BAA;*
- *Maintain ePHI only on encrypted devices.*

HIPAA Hotline 214-456-4444

Think HIPAA's No Big Deal?

$2.5Million fine - Stolen laptop with ePHI of 1391 individuals

- No risk assessment or risk management processes in place
- No policies or procedures for mobile devices
- Security Rule policies ALL in draft form!

Focus on Encryption & Safeguards

Think HIPAA's No Big Deal?

- A physician attempted to deactivate a personally owned computer which opened up a Covered Entity's network firewall, allowing internet access to PHI
- A University & its affiliated hospital paid **$4.8Million** for that failure

Think HIPAA's No Big Deal?

- What's the cost of a lost or stolen laptop?
- Encrypted: $0 in fines
- Unencrypted: **$3.9Million** paid when 1 laptop with information on 13,000 research patients was stolen

Think HIPAA's No Big Deal?

$2.75 Million settlement for **failure to:**

- Restrict workstation access to only authorized users;
- Assign a unique user identity in systems containing ePHI;
- Implement policies & procedures to prevent, detect, contain and correct security violations;
- Have sufficient data to appropriately notify each individual if their PHI had been breached.

Think HIPAA's No Big Deal?

$2,140,500 settlement

- ePHI of 31,800 people left open to the internet for a little over a year
- Failure to recognize the risk of a new server
- No enterprise-wide Risk Assessment

Think HIPAA's No Big Deal?

- A firewall is of little value if everything isn't behind it.
- A health plan paid **$1.7Million** in fines because a weakness in 1 program left their network and the ePHI of over 600,000 individuals open to the internet!

Focus on the Basics

Think HIPAA's No Big Deal?

$5.5Million for failure to provide reasonable access controls resulting in impermissible access to PHI of over 115,000 individuals:

- *Did NOT turn off access for a former employee of an affiliated physician practice*
- *Did NOT monitor access to ePHI*

Think HIPAA's No Big Deal?

- **$2.4Million** plus a Corrective Action Plan
  - *Appropriate notice to Law Enforcement of patient involved in possible medical identity fraud*
  - ***Inappropriate** release of the story, including the patient's identity, in a press release!*

Think HIPAA's No Big Deal?

- A NYC hospital paid ***$2.2Million*** for:
  - *Permitting disclosure of PHI on 2 patents without an authorization while filming a TV program;*
  - *Permitting unrestricted access by the film crews to the facility increasing the likelihood of other inappropriate disclosures.*

Think HIPAA's No Big Deal?

- Failure to have Business Associate Agreements with vendors who have access to PHI have resulted in recent settlements of **$750K** and **$1.55M**!

Think HIPAA's No Big Deal?

- PHI must be protected when it travels!
- A clinic schedule and encounter forms were left on a Boston subway by a hospital employee
- **$1Million** fine was paid by the hospital

Think HIPAA's No Big Deal?

- Failure to provide appropriate notice of lost PHI of 836 individuals contained on paper schedules within the required 60 days
  - *Individuals*
  - *Media*
  - *Office for Civil Rights*

$475,000 Paid

Think HIPAA's No Big Deal?

- Patient requested information be sent to a personal post office box. Provider instead faxed PHI to his employer, including
  - *HIV status*
  - *Mental health history*
  - *Sensitive diagnoses*

$387,000 Paid

Think HIPAA's No Big Deal?

Office for Civil Rights Audit Updates

Think HIPAA's No Big Deal?

- Phase II audits of Covered Entities are Complete
- Phase II audits of Business Associates are in final steps
- There were no onsite audits in Phase II—these were only desk audits
- The Phase III will include onsite audits

Think HIPAA's No Big Deal?

- There will be a summary report to follow the completion of the Phase II audits—it could be published as early as this year
- None of the Phase II audit respondents were moved to the Compliance (Penalty) track
- There were an unknown small number of audit candidates who elected not to respond to the desk audit—these facilities are in the Compliance (Penalty) track

Think HIPAA's No Big Deal?

- The HHS Deputy Director Devin McGraw commented on the state of upcoming guidance
- There will be forthcoming additional guidance on Minimum Necessary and the sharing of settlement payments with patients
- She does not expect OCR to release updated guidance on Accounting of Disclosures anytime in the near future

Think HIPAA's No Big Deal?

What's next?

- keep up to date through enforcement trends
- Watch for news releases (OCR listserve)
- Communicate with leadership on risks
- Have a plan, execute and document

Questions?

Thank you!

Joan M. Podleski, CHRC, CCEP, CHPC
Chief Privacy Officer,
Children's Health, Dallas

R. Brett Short, CHC, CHPC
Chief Compliance Officer
UK Healthcare, University of Kentucky