Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Overview and Addressing Privacy in a New Era of Enforcement

The Sixth HIPAA Summit West

October 10, 2012

Adam Greene, J.D., M.P.H.

WELCOME

Housekeeping

The Dangerous Myth

- The Myth – Nothing new has happened with HIPAA; we don't need to do anything until the Omnibus rule is published

- The Reality – Privacy and security are becoming increasingly important and challenging

Time for the Training Wheels to Come Off

- December 28, 2000 – HHS publishes HIPAA Privacy Rule
- April 14, 2003 – Compliance deadline for Privacy Rule
- July 16, 2008 – First HIPAA settlement
- February 17, 2009 – HITECH Act directs HHS to penalize all violations due to “willful neglect”
- December 2012 - HIPAA privacy and security audits begin

Privacy and Security Continues to Change

- New challenges:
  - Mobile devices
  - Cloud computing
  - EHR adoption
- Increased liability:
  - Breach notification exposure
  - Increased enforcement
- Same old problems
  - Forever curious employees

HHS Enforcement Starts to Trickle

- Number of HHS settlements/ CMPs have slowly increased
  - 2003-2007: None
  - 2008: One
  - 2009: One
  - 2010: Two
  - 2011: Three
  - 2012 (so far): Four
- Average settlement: ~ $1 Million
- CMP - $4.3 Million

States Increase Enforcement Efforts

- 2010 – Connecticut settles with Health Net for $250,000
- 2011 – Vermont settles with Health Net for $55,000
- 2011 – Indiana settles with Wellpoint for $100,000
- 2012 – Mass. settles with $475,000
- 2012 – Minn. settles with Accretive Health for $2.5 million

California Privacy Penalties

- 19 penalties imposed
- 16 facilities
- Average penalty of $133,000
- Total penalties of $2.5 million
- Most (14) fines related to unauthorized access by employees

Class-Action Lawsuit Frenzy Begins

- “Health Net Inc. and IBM face a class-action lawsuit seeking $5 million in damages over the loss of computer storage devices ….”
- “A class-action lawsuit seeking as much as $16 million … over a data breach … at the UCLA Health System.”
- “11 class-action lawsuits against Sutter Health over a data breach are being consolidated … could amount to between $944 million and $4.25 billion total, not including attorneys' fees and court costs.”

Cheer Up!

- There are steps you can take…

Update your Privacy Program

Focus on Continuous Compliance

Assess Privacy Policies and Procedures

- Privacy Rights
  - Are patients actually receiving notices of privacy practices?
  - Are all requests for restrictions considered?
  - When are requests for alternative communications “reasonable”?
  - Are access/amendment requests recognized and timely handled?
  - Are disclosure logs maintained?

Assess Privacy Policies and Procedures

- Uses and Disclosures
  - Do policies address recurring categories of uses and disclosures?
  - Do procedures prove effective in real world situations?
  - Have minimum necessary policies been created for routine requests, uses, and disclosures?
  - Are minimum necessary criteria applied to nonroutine requests, uses, and disclosures?

Assess Privacy Policies and Procedures

- Breach Notification
  - Can all members of the workforce identify a breach
  - Do policies and procedures provide a clear path for notification within the organization?
  - Are there objective criteria for judging what constitutes a breach?

Evaluate Training

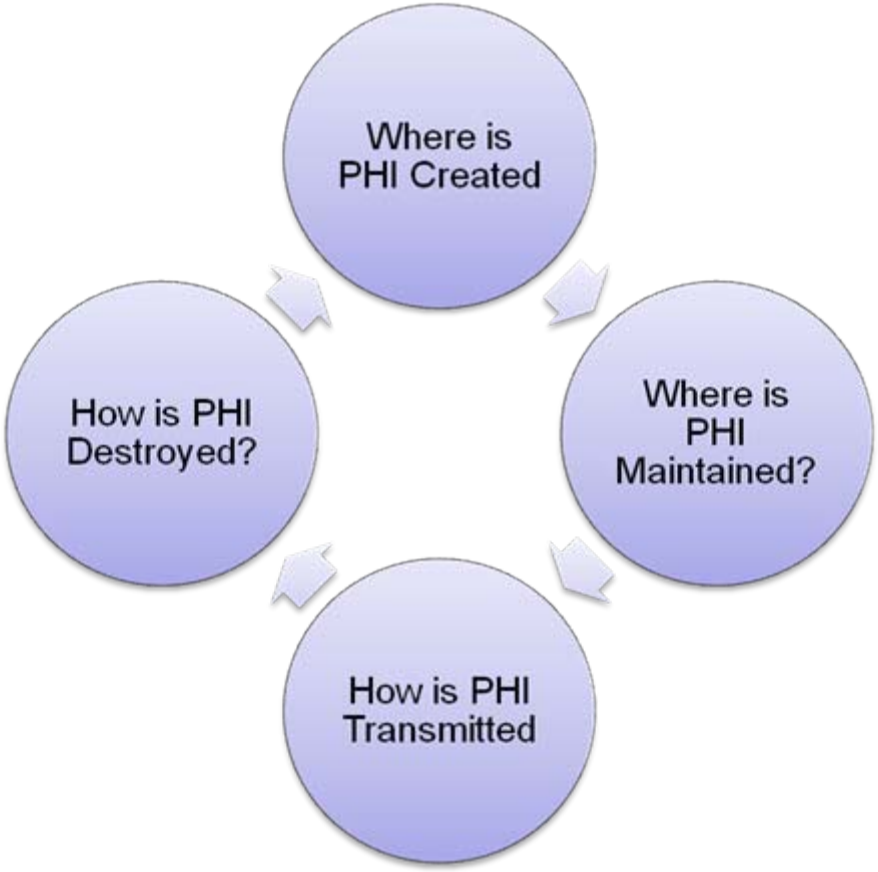
- Does training adequately cover all policies?
- Is training tailored to issues arising in your organization?
- Is training broken up if necessary?
- Does training focus on real-world situations?

Enforce Consequence for Noncompliance

- Noncompliance should have consequences … for all members of the workforce.
- Sanctions policies can have flexibility to handle different levels of noncompliance.
- Sanctions experience can inform policies, training, and safeguards.

Auditing Effectiveness

Follow the PHI



Auditing Effectiveness

- Some procedures will not work – you need to discover this before patients or the government.
  - Do employees understand training?
  - Is PHI being properly maintained at workstations?
  - How is PHI actually disposed?

Document, Document, Document

- Policies and procedures (new and old)
- Patient privacy requests
- Complaint investigations
- Training (substance and certifications)
- Sanctions (including any retraining/counseling)
- All safeguards

Questions

For more information

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213