Addressing Privacy in a New Era of Enforcement

The 20th National HIPAA Summit

March 26, 2012

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

Davis Wright Tremaine LLP

DEFINING SUCCESS TOGETHER

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

Formal Enforcement Starts to Trickle

- 2010-2011 – HHS reaches four settlements and issues one CMP (up from only two before 2010)
- CT, VT, and MN attorneys general bring enforcement actions under HITECH Act
- State governments (e.g., CA) get more aggressive under state law

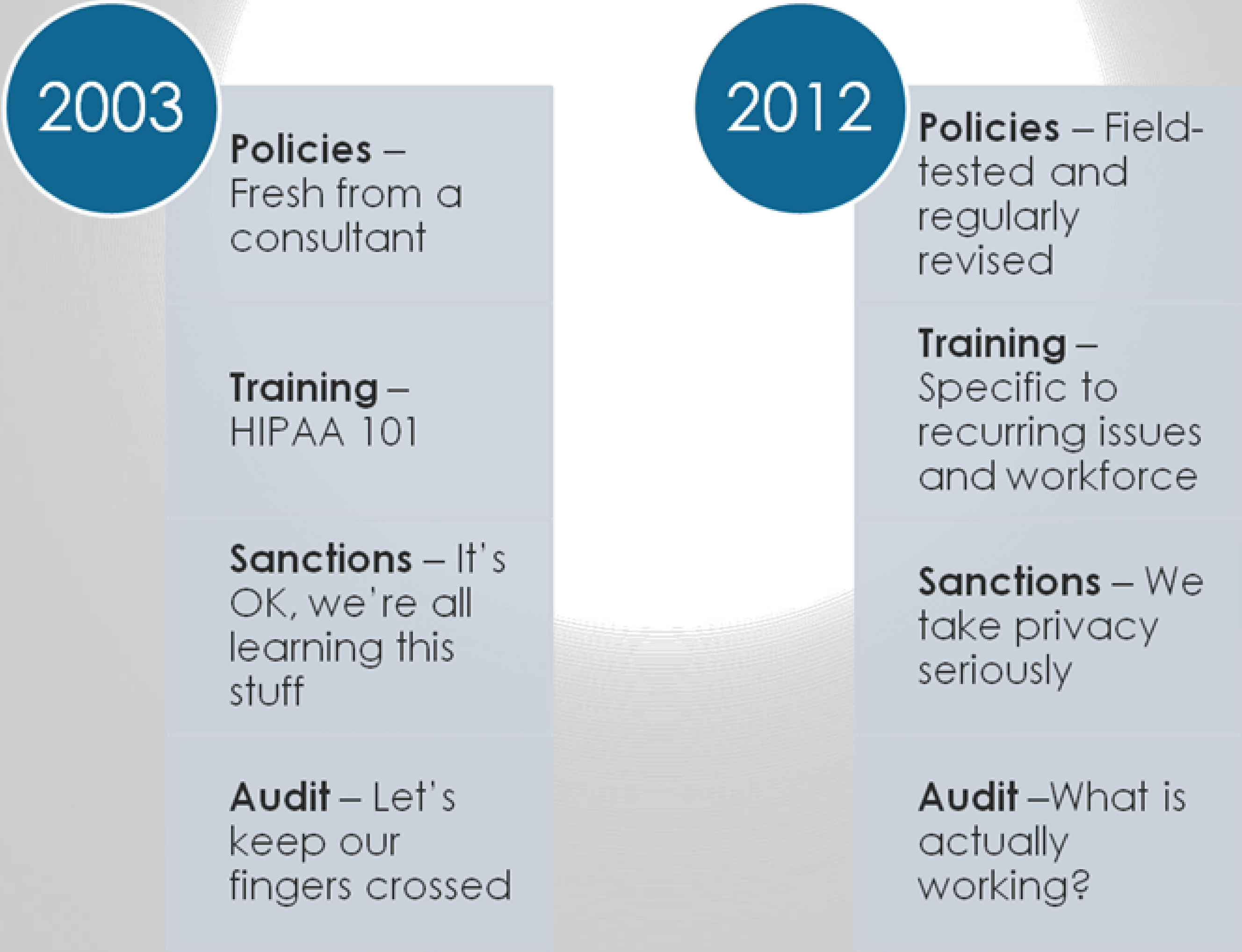
Class-Action Lawsuit Frenzy Begins

- "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!

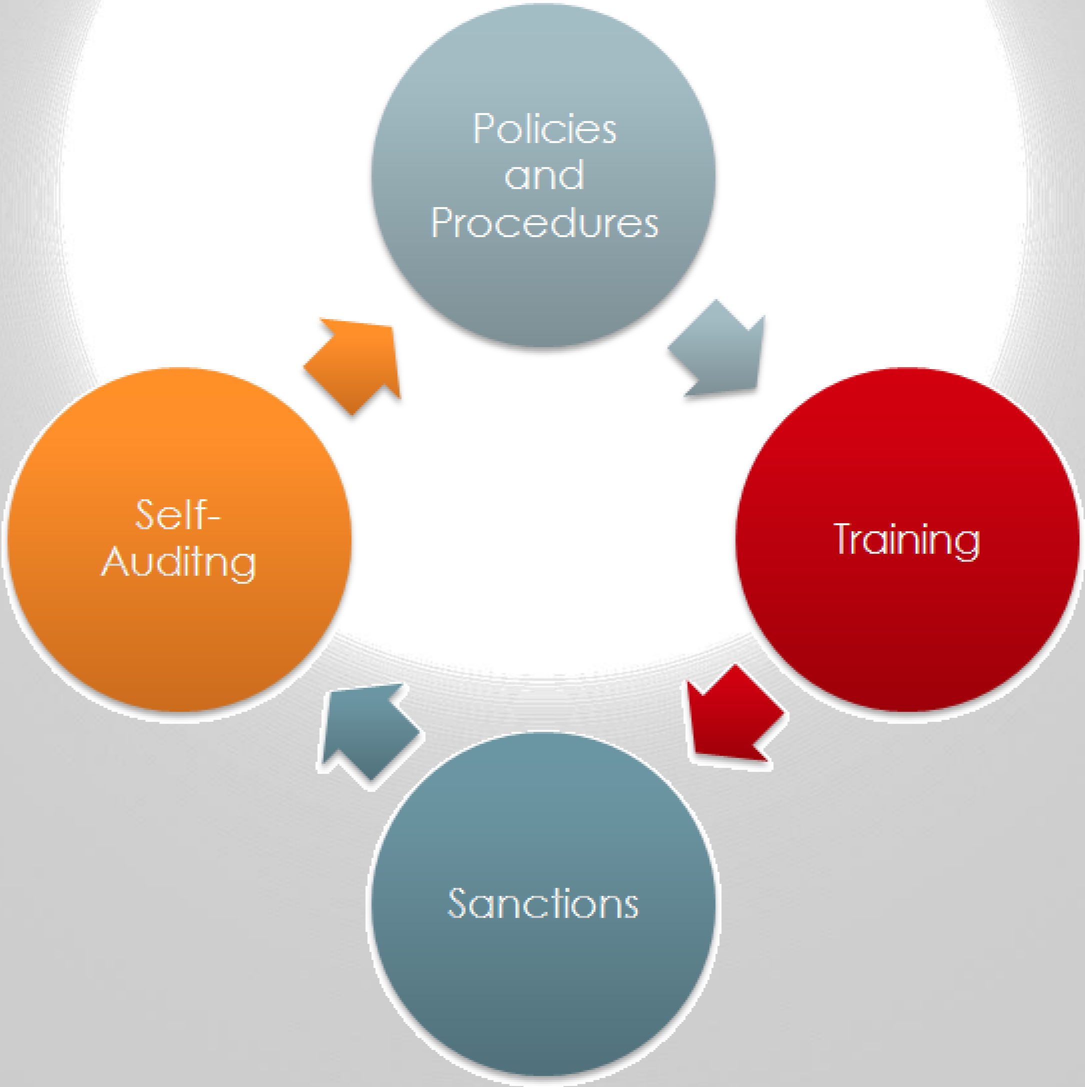
- There are steps you can take…

Update your Privacy Program



2003	2012
Policies – Fresh from a consultant	**Policies** – Field-tested and regularly revised
Training – HIPAA 101	**Training** – Specific to recurring issues and workforce
Sanctions – It's OK, we're all learning this stuff	**Sanctions** – We take privacy seriously
Audit – Let's keep our fingers crossed	**Audit** –What is actually working?

Focus on Continuous Compliance



Policies and Procedures

Training

Sanctions

Self-Auditng

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
  - 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 basic concepts?
- Is training tailored to issues arising in your organization?
- Does training focus on issue spotting (e.g., potential breach)?
- Does training focus on real-world situations?

Enforce Consequence for Noncompliance

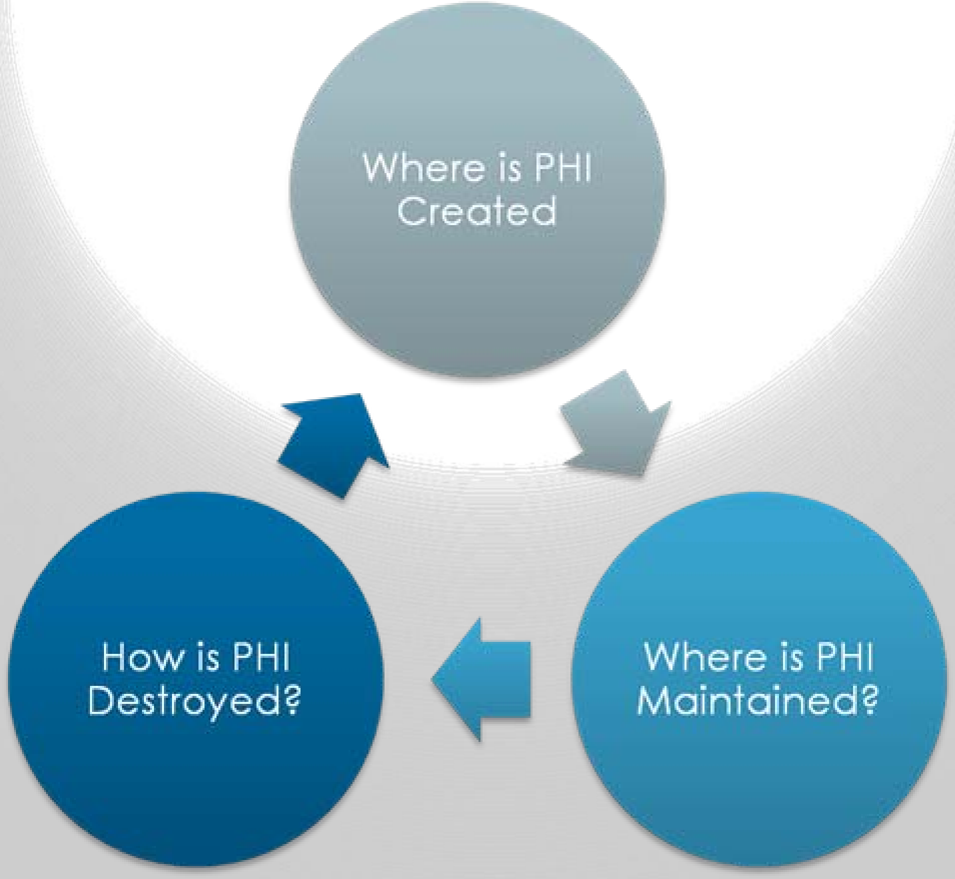
- Noncompliance should have consequences … for all members of the workforce.

- Sanctions policies can have flexibility to handle different levels of noncompliance.

- Sanctions experience can inform policies, training, and safeguards.

Auditing Effectiveness

Follow the PHI



Where is PHI Created

Where is PHI Maintained?

How is PHI Destroyed?

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