HIPAA Administrative Simplification

Integrating Privacy and Security

William R. Braithwaite, MD, PhD
"Doctor HIPAA"
Bill@Braithwaites.com

HIPAA Summit/WEDI Security

Baltimore, MD

September 14, 2004

Purpose of HIPAA Administrative Simplification Subtitle

- "To improve the efficiency and effectiveness of the health care system
  - by encouraging the development of a health information system
  - through the establishment of standards and requirements for the electronic transmission of certain health information."

HHS Required to Adopt Standards:

- Electronic transmission of specific administrative and financial transactions
  (including data elements and code sets)
  - List includes claim, remittance advice, claim status, referral certification, enrollment, claim attachment, etc.
- Unique identifiers (including allowed uses)
  - Health care providers, plans, employers, & individuals.
- Security and electronic signatures
  - Safeguards to protect health information.
- Privacy
  - For individually identifiable health information.

HIPAA ASS Extended Timeline

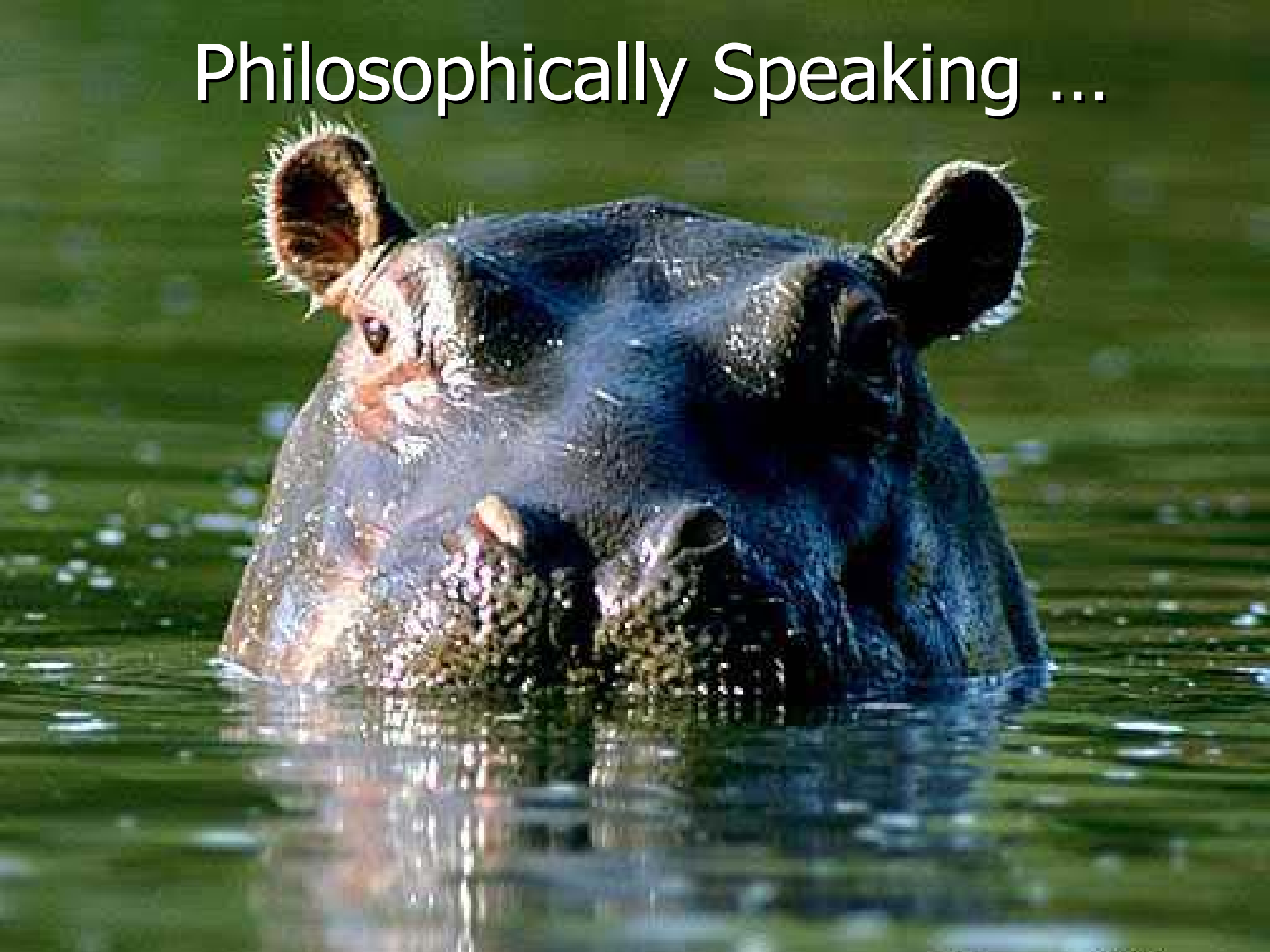
- Legislation written – 1994
- Law Passed – 1996
- First proposed regulation – 1998
- First final regulation – 2000
- First implementation date – 2003
- Last implementation date – 2010 +

What's privacy?

Definitions for Privacy & Security

- Privacy is the right of an individual to
  - control your own personal information, and
  - not have it disclosed or used by others without permission.
- Confidentiality is the obligation of another party to respect privacy by
  - protecting personal information they receive, and
  - preventing it from being used or disclosed without the subject's knowledge and permission.
- Security is the means used protect the confidentiality of personal information through
  - physical, technical and administrative safeguards.

Philosophically Speaking ...



Principles of Fair Info Practices

- Notice
  - Existence and purpose of record-keeping systems must be known.
- Choice – information is:
  - Collected only with knowledge and permission of subject.
  - Used only in ways relevant to known purpose.
  - Disclosed only with permission or overriding legal authority.
- Access
  - Individual right to see records and assure quality of information.
    - accurate, complete, and timely.
- Security ->
  - Reasonable safeguards for confidentiality, integrity, and availability of information.
- Enforcement
  - Violations result in reasonable penalties and mitigation.

BE REASONABLE! (265 times)

Safeguards in Privacy Rule

- A covered entity must:
  - have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI).
  - reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the [privacy] standards, implementation specifications or other requirements ….
  - reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Specific Security in Privacy

- Role-based access required under minimum necessary rule.
- Verification and authentication of individuals and authorities requesting PHI.
- Security required by Privacy Rule applies to all PHI in all forms, including oral and paper.
  - Final Security Rule only applies to electronic information.


E-LEARNING 132 · NEW ECONOMY FLAMEOUT 146 · MULTILINGUAL SITES 162
JANUARY 15, 2001
NINE DOLLARS
CIO
The Magazine for Information
WHY PACKAGED SOFTWARE STINKS— WHAT YOU CAN DO ABOUT IT
PAGE 108
FEDS EYE INDUSTRY EXCHANGES— CLOUDY SKIES FOR ORBITZ?
PAGE 122
ROBERT REICH ON ANGST, ALIENATION AND THE NEW ECONOMY
PAGE 156
Are your medical secrets Safe?
CIOs are working overtime to balance security with access. Call it The Privacy Problem. PAGE 75
Plus, Do You Need a CPO? PAGE 88
CareGroup CIO John Halamka

What happens on an average weekend?

CareGroup Inbound Data Traffic Factoids:

after 5p on Fridays and before 8.30a on Mondays

11,892,210 internet-sourced packets aimed at specific CareGroup port numbers were blocked. (All these ports were open before the Firewall Project started.)

9,922,303 packets were permitted into port 80-http and port 443-https

4,187,689 lookups against corporate DNS servers occurred

1,958,892 packets were permitted inbound to port 25-smtp email hosts

220,588 packets were permitted inbound to various hosts supporting pcAnywhere connections

114,271 packets were addressed to port-23 telnet hosts located within CareGroup

91,176 ping attempts were blocked

62,270 echo-reply/traceroute requests were blocked

61,330 packets inbound were permitted to the CareGroup port 110-POP server

59,463 blocked probes were logged looking for open smtp ports on hosts other than permitted ones

44,328 packets of IPSEC Triple-DES VPN tunneling were logged into CareGroup

30,994 packets were permitted inbound to Macintosh hosts supporting remote Timbuktu connections

21,923 packets transferred into CareGroup hosts via port–21 ftp connections sourced inside CareGroup.

18,243 DICOM packets entered CareGroup for BID PACS

Bare Bones of HIPAA Security

Key Security Rule Philosophy

- Identify & assess organizationally specific risks/threats to electronic PHI:
  - **Availability**
  - **Integrity**
  - **Confidentiality**
- Take reasonable steps to reduce risk.
- Involves policies/procedures & contracts with business associates more than technology.
  - **For security technology to work, behavioral safeguards must also be established and enforced.**
    - **requires administration commitment and responsibility.**

Final Security Rule

- Definitions and applicability harmonized with privacy.
- Organization specific risk analysis and documentation of decisions.
- Only applies to electronically maintained and transmitted health information.
  - Rules for non-electronic PHI may come later.
- Technology neutral.
- No electronic signature standard.

Security standards: General rules

- A covered entity (CE) must:
  - Ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits.
  - Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
  - Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the privacy rules.
  - Ensure compliance by its workforce.

Security Rule Structure

- Rule composed of 18 standards, each of which may have required and addressable implementation specifications (ISs).
- CE must comply with all the standards with respect to all electronic PHI.
- Review and modify security measures as needed to continue reasonable and appropriate protection of electronic PHI.

ISs: required or addressable.

- CE must implement Standards & required ISs.
- CE must assess addressable ISs to see if they are reasonable and appropriate
  - when analyzed as to their contribution to protecting electronic PHI; and
    - implement them if reasonable and appropriate; and
    - if implementing one is not reasonable and appropriate:
      - document why it would not be reasonable and appropriate to implement; and
      - implement an equivalent alternative measure if reasonable and appropriate.

Security standards: Flexibility

- CE may use any security measures that allow it to reasonably and appropriately implement the standards and ISs.
- CE must take into account:
  - The size, complexity, and capabilities of the covered entity.
  - The covered entity's technical infrastructure, hardware, and software security capabilities.
  - The costs of security measures.
  - The probability and criticality of potential risks to electronic PHI.

BE REASONABLE! (72 times)

Didn't we DO this for Privacy???

- Administrative Safeguards are similar, compatible, and complimentary.
- Need to understand your information environment to control and protect it.
- Need top-down commitment to implement successful data protection programs.
  - Privacy was new, got attention and funding.
  - Security has been around, IT shop handles that!

Know your data! (URAC Standard)

- The organization has completed an assessment of its PHI uses and disclosures. The assessment addresses the following issues:
  - The types and sources of PHI received or generated by the organization;
  - Where and how PHI is stored;
  - The internal users of such information, and the purposes of such use;
  - Routine external requests for and disclosures of such information, and the purposes of such disclosures; and
  - Non-routine external requests for and disclosures of such information, and the purposes of such disclosures.

How do I compare thee?

Privacy & Security Similarities

- Intended to be compatible.
- Common Applicability & Administrative Requirements.
- Both provide workforce access controls and protections.
- Both require BA contracts with vendors.
- Both require modifications to group health plan documents.
- Both require 'reasonable' measures (despite "ensure").
- Similar sanction and mitigation requirements.
- Same approach to ACEs and hybrids.

Administrative Requirements

- Apply to both privacy and security.
- Flexible & scalable (i.e., requires thought!).
- Covered entities required to:
  - Designate a responsible official (privacy/security).
  - Develop written policies and procedures (including on receiving complaints).
  - Provide training to its workforce.
  - Develop a system of sanctions for employees who violate the entity's policies.
  - Meet documentation requirements.

Privacy & Security Differences

- Privacy safeguards cover PHI in all media;
  - Security only covers electronic media.
  - Potential for non-electronic security rule in future.
- Privacy includes explicit, detailed instructions.
  - Security more flexible, more dynamic based on risk analysis/management, monitoring, and periodic review.
- Different enforcement agencies and penalties.
- Enforcement rules incomplete – mostly address privacy.
- Privacy has exceptions for incidental uses and disclosures.
- Security advises audit trails (internal)
  - Privacy limited to supporting patient requests for accounting of disclosures (external).
- Security has no OHCA – BAA may be required for security.
- Preemption – more stringent state law doesn't apply to security (IF it is contrary!).

What are the Major Barriers?

4 key stumbling blocks (URAC)

- Incomplete or inappropriately scoped ***risk analysis***.
  - does the health care organization understand whether or not patient data is at risk of compromise on their systems?
- Inconsistent and poorly executed ***risk management***.
  - does the health care organization actively address the technical issues and employee practices that affect security?
- Limited or faulty ***information system activity review***.
  - does the health care organization actively collect data on how its systems and employees are performing?
- Ineffective ***security incident reporting and response***.
  - does the health care organization even detect when patient data has been compromised (e.g., stolen by an unauthorized person) and how do they deal with that compromise?

Risk Analysis

- Risk Analysis is the fundamental building block.
  - formal identification of the organization's risk tolerance, its outstanding risk liabilities or residual risk, and a prioritization of subsequent risk reduction activities.
- When investigating security complaints, the Risk Analysis will be a primary piece of evidence that the government will use to evaluate the organizations due diligence and rationale for reasonable and appropriate controls.
- Contrary to what many in the security industry have promoted, Risk Analysis as required by the Security Rule is a much more demanding evaluation of the organization's security posture than that afforded by a typical vulnerability assessment.

Risk Management

- Security Risk Management is about allocating resources to gain the highest level of risk reduction possible within the bounds of an organization's risk tolerance.
  - Does the health care organization have a process to actively address the technical issues and employee practices that affect security?
- Organizations must be careful not to overly rely on technologists to make risk management assumptions without clear guidance and support from the business operations perspective.
- All of the organizations surveyed were found to have serious issues with policy and procedure documentation, management, and implementation.

Information System Activity Review

- Information System Activity Review is an essential element of the security risk management equation.
  - Does the health care organization actively collect and review data on how its systems and employees are performing?

Security Incident Response and Reporting

- What constitutes a security incident and what constitutes a sufficient level of reporting?
  - Does the health care organization even detect when patient data has been compromised (e.g., stolen by an unauthorized person or entity) and how do they deal with that compromise?

Who's Responsible?

Additional Demands for Security

- HIPAA Privacy Rule;
- Professional liability insurance;
- Contracting RFP/RFI requirements;
- Federal security requirements;
- URAC accreditation standards; and
- Growing expectations for security by patients, providers, and other stakeholders.

Security is a Business Risk!

- Organizations should incorporate the oversight of security risks into their overall business risk management programs.
  - Potential for efficiency, protection from liability exposures, and cost savings
  - Creation of a security "due diligence" package that presents a single vision of business risk, including security posture, to all stakeholders.
  - Standard of Due Care
    - gives organizations opportunity to meet their "due care" responsibilities in an efficient and cost effective manner.
  - Keeping Up with the Norm
    - Health care inextricably linked to security efforts in other industries.
  - Managing Internal Expectations
    - 6 months to 1 year to design and implement

What's the Bottom Line?

Bottom Line

- Adequate security is essential to support adequate privacy.
  - As well as an essential business practice.
- Privacy policies and procedures guide implementation of security (confidentiality).
  - Security (availability and integrity) requirements feedback into privacy policies and procedures.
- A breach is likely to involve violations of both sets of rules.
- A common organizational approach to privacy and security (Information Protection Program) has merit.

Questions?

- CMS web site www.cms.hhs.gov/hipaa/hipaa2.
- OCR web site www.hhs.gov/ocr/hipaa/
- NIST Special Publication 800-66 www.nist.gov
- Security and Privacy White Papers www.wedi.org/snip/

"William" is a bright blue, 8 inch, Egyptian hippopotamus located in the Metropolitan Museum of Art. He is made of faience, a ceramic material, and is decorated with lotus blossoms, which represent the hippo's creative forces in nature.

- Bill@Braithwaites.com