

# WEDi



HIPAA Security and Privacy  
Rules: Working together

***HIPAA SUMMIT WEST 2001***  
***June 21, 2001***

Tom Hanks - WEDi  
Co-chair Privacy Policy Advisory Group  
Co-chair Security Policy Advisory Group



# Working Together: HIPAA Security and Privacy

---

- ◆ Security NPRM
- ◆ Privacy Rule – final 4/14/2001
- ◆ Final Security rule will be harmonized with the final Privacy rule
- ◆ Final Privacy rule prepares us for the final Security rule



# Working Together: HIPAA Security and Privacy

---

- ◆ Who & what is covered
- ◆ Reasonableness – how much is enough
- ◆ Audit trails
- ◆ Areas of protection



# Working Together: HIPAA Security and Privacy

---

- ◆ Scalability of requirements
- ◆ Access controls
- ◆ Internal use & disclosure
- ◆ What kind of “safeguards” are required



# Security vs. Privacy... Definitions

---

## ◆ Security

–ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss



# Security vs. Privacy: Definitions

---

## ◆ Privacy

- defines who is authorized to access information (the right of individuals to keep information about themselves from being disclosed)
- Individual's rights



# DHHS Privacy & Security Rules Commonalities

---

- ◆ Boundaries
  - Who & what is covered
- ◆ Security: Safeguarding PHI
- ◆ Administrative
  - Policies & procedures





# Security – What is Covered Protected Health Information

---

## ◆ Security

- Any individually identifiable health information maintained or transmitted electronically
- Also includes demographics





# Privacy – What is Covered Protected Health Information

---

- ◆ Privacy - Broader Definition of Protected Health Information
  - All individually identifiable health information in ANY form or media
  - Includes subsets of health information such as demographics



# Privacy – Defines Identifiable

---

- ◆ De-identified data defined by removing list of elements
- ◆ Statistical determination that the risk of re-identification by the receiving entity is very small



# Privacy and Security— Who Are Covered Entities

---

- ◆ Clearinghouses
- ◆ Health Plans
- ◆ Health care providers that transmit covered transactions



# Privacy – Expands the Boundaries of Protection

---

- ◆ Business Associate Contract (BAC) required with any entity that performs services to or on behalf of a covered entity that uses or discloses PHI belonging to the covered entity.



# Privacy – Expands the Boundaries of Protection

---

- ◆ BAC requires the business associate to maintain safeguards necessary to protect PHI from unauthorized disclosure
- ◆ Final Security rule conforming to Privacy BA provisions



# Security – Safeguarding PHI

---

- ◆ Establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information
- ◆ Requirements are technology neutral - - each organization determines the technology to achieve outcome



# Security – Safeguarding PHI (cont'd)

---

- ◆ No proscribed implementation
- ◆ Reasonably required to protect from intentional or unintentional violation
- ◆ Each health care business determines their own needs
- ◆ Implementation varies according to size and type of entity
- ◆ Must consider cost





# Privacy – Safeguarding PHI

---

- ◆ Must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI
- ◆ Reasonably safeguard health information



# Privacy – Safeguarding PHI Reasonably?

---

- ◆ Common sense, flexible and scalable
- ◆ Implementation varies with size and type of activities
- ◆ Must consider cost
  - Strike a balance between protecting privacy and the cost of doing so



# Privacy – Safeguarding of PHI

---


- ◆ Not required to guarantee the safety of PHI against all threats
- ◆ Theft of PHI may not be a violation if reasonable policies in place



# Security – Need to Know Provision

---

Need-to-know procedures for personnel access (a security principle stating that a user should have access only to the data he or she needs to perform a particular function).



# Privacy - Minimum Necessary Provision

---

Except for treatment...

- Disclosure of any patient information is limited to the minimum amount necessary to accomplish the purpose of the disclosure
- Internal & external



# Security – Access Controls

---

- ◆ Context based
- ◆ User based
- ◆ Role based



# Privacy – Access Controls

---

- ◆ Privacy rule establishes access
- ◆ Role based
- ◆ Identify persons or class of persons that need access to PHI
- ◆ Limit access to only the PHI needed to perform their job





# Privacy – Access Controls Reasonable Efforts

---

- ◆ Takes into account the ability of the entity to configure its record system to allow selective access
- ◆ Practicality of organizing systems to allow this capacity
- ◆ Recognizes limitations on parsing paper records



# Security – Audit Trails

---

- ◆ Audit trails required – no implementation provision
- ◆ The data collected and potentially use to facilitate a security audit
- ◆ Internal audit requirement to review records of system activity – audit trail



# Privacy – Accounting for Disclosure – No Audit Trail

---

1. Date of each disclosure
2. Name and address, if known, of person or entity receiving the PHI
3. Brief description of information disclosed
4. Purpose for disclosure or copy of individual's authorization



# Privacy – Defines Audit Trail Expectations

---

- ◆ Audit trails do not usually record each time a record is used or reviewed
- ◆ Audit trails typically record each time a sensitive record is altered
- ◆ Important to coordinate Accounting for Disclosure with Audit Trails in Security



# Security – Training Requirements

---

- ◆ Security awareness training
  - All employees, agents and contractors
  - Customized to job responsibilities
  - Focus on issues: e.g. use of PHI, confidentiality and security
  - Specifics such as: password management, virus control and incident reporting
  - On-going reminders



# Privacy – Training Requirements

---

- ◆ Provide training to entire workforce
  - Policies and procedures used to protect PHI under Privacy
  - Completed by compliance date and then for all new members of workforce Re-train affected employees on any changes in privacy policies
  - Policies and procedures must be implemented to both provide training and document completion





# Security – Policies & Procedures

---

- ◆ General security policies
- ◆ Audit, assessment & risk analysis
- ◆ Audit trails & monitoring
- ◆ Change control Media controls
- ◆ Contingency planning and disaster recovery





# Security – Policies & Procedures

(cont'd)

---

- ◆ Termination and orientation
- ◆ Access controls
- ◆ Personnel clearance
- ◆ Formal record processing
- ◆ Security incident
- ◆ Workstation location



# Privacy – Policies & Procedures

---

- ◆ Reasonably designed and developed to comply with rule - taking into account size and nature of the activities
- ◆ Documented in writing – keep for 6 years



# Privacy – Policies & Procedures

(cont'd)

---

- ◆ Process in place for revision to promptly reflect changes in applicable laws or regulations
  - Ensure that revisions of privacy practices comply with the Privacy rule and that revisions are promptly reflected in privacy policies
  - Process to revise notices and inform individuals of the revision



## Wrap-Up

- ◆ Security & Privacy rules are interwoven
- ◆ Both Security and Privacy address safeguarding health information
- ◆ No material changes to Security NPRM expected
- ◆ Final Security rule is being aligned with final Privacy rule
- ◆ Final Privacy rule gives us guidance to what to expect from final



## Resources

---

- ◆ WEDI web site
  - [www.wedi.org](http://www.wedi.org)
- ◆ AFEHCT web site
  - [www.afehct.org](http://www.afehct.org)
- ◆ EHNAC web site
  - [www.ehnac.org](http://www.ehnac.org)



## Resources

---

- ◆ DHHS - administrative simplification
  - [aspe.dhhs.gov/admnsimp/index.htm](http://aspe.dhhs.gov/admnsimp/index.htm)
- ◆ DHHS data council web site
  - [aspe.dhhs.gov/datacncl/](http://aspe.dhhs.gov/datacncl/)
- ◆ NCVHS Web Site
  - [ncvhs.hhs.gov](http://ncvhs.hhs.gov)



## Resources

---

- ◆ HIPAA Comply web site
  - [www.HIPAAcomply.com](http://www.HIPAAcomply.com)
- ◆ HIPAAAlive web site
  - [www.HIPAAAlive.com](http://www.HIPAAAlive.com)



# OWED!

Thank you!



*Tom Hanks*

*630.514.7706*

*TomHanks@ameritech.net*