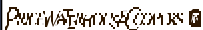







HIPAA	
Privacy and Security - Common Concepts	
HIPAA COW	
January 24, 2003	
Tom Hanks National Director Client Services Health Care Practice Tom.Hanks@us.pwcglobal.com 	



Working Together: HIPAA Security & Privacy	
	<ul style="list-style-type: none"> ▪ What is covered/protected ▪ Reasonableness – how much is enough ▪ Areas of protection ▪ Enforcement
Copyright © 2002 PricewaterhouseCoopers LLP 	




Security vs. Privacy - Definitions	
	<p>Security</p> <ul style="list-style-type: none"> • Ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss
Copyright © 2002 PricewaterhouseCoopers LLP 	



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

Copyright © 2002 PricewaterhouseCoopers LLP



Privacy - What is Protected

- **Privacy – broad protection of Protected Health Information (PHI)**
- **Covers all individually identifiable health information in ANY form or media**
- **Requires safeguards be in place to protect the privacy of all PHI**
 - Includes subsets of health information such as demographics


Copyright © 2002 PricewaterhouseCoopers LLP



Privacy - What is Protected (cont'd)

- **Privacy Modification Rule (PMR) Confirms Security Requirements**
 - Privacy requires safeguards for ALL PHI
 - Security will address only PHI maintained or transmitted electronically
 - Safeguards to protect privacy of All PHI in place by April 14, 2003

Copyright © 2002 PricewaterhouseCoopers LLP




Privacy

- Expands Protection (cont'd)

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

Copyright © 2002 PricewaterhouseCoopers LLP






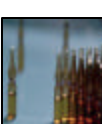
Security NPRM

- What is Protected

- **Security rule is limited in scope**
- **Covers safeguard requirements ONLY for PHI maintained or transmitted electronically**

Copyright © 2002 PricewaterhouseCoopers LLP



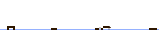



Security NPRM

- Safeguarding PHI

- **Establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information**

Copyright © 2002 PricewaterhouseCoopers LLP




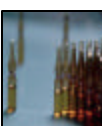


Security NPRM - Safeguarding PHI (cont'd)

- 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

Copyright © 2002 PricewaterhouseCoopers LLP



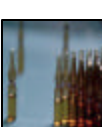


Security NPRM - Safeguarding PHI (cont'd)

- Requirements are technology neutral – each organization determines the technology to achieve outcome

Copyright © 2002 PricewaterhouseCoopers LLP

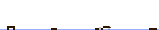





Privacy - Safeguarding PHI

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

Copyright © 2002 PricewaterhouseCoopers LLP







Privacy

- Safeguarding PHI (cont'd)

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

Copyright © 2002 PricewaterhouseCoopers LLP






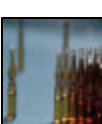
Privacy

- Safeguarding PHI (cont'd)

- **Not required to guarantee the safety of PHI against all threats**
- **Theft of PHI may not be a violation if reasonable policies in place**
- **Note: PMR explicitly permits certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure**

Copyright © 2002 PricewaterhouseCoopers LLP



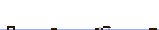



Security NPRM

- Access Controls

- **Need to know procedures for access control**
 - Context based
 - User based
 - Role based

Copyright © 2002 PricewaterhouseCoopers LLP






Privacy - Minimum Necessary

- **Except for treatment...**
 - Disclosure of any patient information is limited to the minimum amount necessary to accomplish the purpose of the disclosure
 - Internal & external
 - **PMR exempts from the minimum necessary standard any uses or disclosures for which the covered entity has received an authorization**

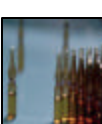
Copyright © 2002 PricewaterhouseCoopers LLP



Privacy - Access Controls

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


Copyright © 2002 PricewaterhouseCoopers LLP



Privacy - Access Controls

- **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**
- **PMR affirms reasonableness position**


Copyright © 2002 PricewaterhouseCoopers LLP




Security NPRM – 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**

Copyright © 2002 PricewaterhouseCoopers LLP




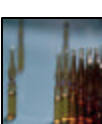


Privacy – Accounting Versus – Audit Trail

- **Date of each disclosure**
- **Name and address, if known, of person or entity receiving the PHI**
- **Brief description of information disclosed**
- **Purpose for disclosure or copy of individual's authorization**
- **PMR removes requirement for disclosures with authorization**

Copyright © 2002 PricewaterhouseCoopers LLP

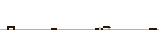




Privacy – Audit Trail Defined

- **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**

Copyright © 2002 PricewaterhouseCoopers LLP



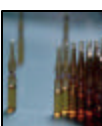


Security NPRM - Training Requirements

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

Copyright © 2002 PricewaterhouseCoopers LLP




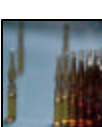


Privacy - Training Requirements

- **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

Copyright © 2002 PricewaterhouseCoopers LLP

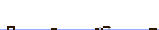





Privacy - Training Requirements (cont'd)

- **Retrain affected employees on any changes in privacy policies**
- **Policies and procedures must be implemented to both provide training and document completion**

Copyright © 2002 PricewaterhouseCoopers LLP







Security NPRM - Policies & Procedures

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

Copyright © 2002 PricewaterhouseCoopers LLP




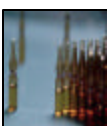


Security NPRM - Policies & Procedures (cont'd)

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

Copyright © 2002 PricewaterhouseCoopers LLP




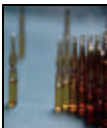


Privacy - Policies & Procedures

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

Copyright © 2002 PricewaterhouseCoopers LLP






Privacy - Policies & Procedures (cont'd)

- **Process in place for revision to promptly reflect changes law**
- **Ensure that revisions are promptly reflected in privacy policies**
- **Process to revise notices and inform individuals of the revision**

Copyright © 2002 PricewaterhouseCoopers LLP





Privacy - Enforcement

- **HHS – Office of Civil Rights**
 - No desire to apply civil/criminal penalties
- **Third party lawsuits**
- **Federal Trade Commission**

Copyright © 2002 PricewaterhouseCoopers LLP





FTC Privacy/Security Microsoft Case

False security and privacy promises related to Passport & Wallet services

"Good security is fundamental to protecting consumer privacy"

– <http://www.ftc.gov/opa/2002/08/microsoft.htm>

Copyright © 2002 PricewaterhouseCoopers LLP





FTC Privacy/Security Microsoft Case

“Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act.”

– Timothy J. Muris, Chairman of the Federal Trade Commission.

Copyright © 2002 PricewaterhouseCoopers LLP





FTC and Health Care - Eli Lilly Case

**Disclosed E-mail Addresses of 669
Subscribers to its Prozac Reminder
Service – August 2002**

"Even the unintentional release of sensitive medical information is a serious breach of consumers' trust."

– <http://www.ftc.gov/opa/2002/01/elililly.htm>

Copyright © 2002 PricewaterhouseCoopers LLP



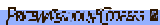


FTC and Health Care - Eli Lilly Case (cont'd)

“Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information.”

– J. Howard Beales, III, PhD - Director of the FTC's Bureau of Consumer Protection.

Copyright © 2002 PricewaterhouseCoopers LLP





FTC and HIPAA

FTC views HIPAA's Privacy Rule requirement to provide Notice of Privacy Practices as a consumer promise - and could respond to consumer complaints of privacy violation – security would be relevant

– J. Howard Beales, III, PhD - Director of the FTC's Bureau of Consumer Protection – Privacy Officers Association Conference, Chicago, IL - November 2002

Copyright © 2002 PricewaterhouseCoopers LLP





Wrap-Up

- **Final Privacy provides guidance on final Security Rule – final Security rule aligned with Privacy rule**
- **Security is required to support Privacy**
- **No material changes to Security NPRM expected**
- **Other concerns may drive security to support privacy**

Copyright © 2002 PricewaterhouseCoopers LLP





Resources

- **PwC Health Care**
- www.pwcglobal.com/healthcare
- **WEDI web site**
 - www.wedi.org
- **AFEHCT web site**
 - www.afehct.org
- **EHNAC web site**
 - www.ehnac.org

Copyright © 2002 PricewaterhouseCoopers LLP





Resources

- **DHHS - administrative simplification**
 – aspe.dhhs.gov/admsimp/index.htm
- **Office of Civil Rights**
 – www.hhs.gov/ocr/hippa
- **NCVHS Web Site**
 – ncvhs.hhs.gov

Copyright © 2002 PricewaterhouseCoopers LLP 



Questions?

Tom Hanks
 National Director Client Services
 Health Care Practice
Tom.Hanks@us.pwcglobal.com

