HIPAA Summit West II

PRECONFERENCE III: Basic Training for Healthcare Privacy & Security Officers

Faculty:
Stephen Cobb, CISSP
Ray Everett-Church, Esq.
Michael Miora, CISSP

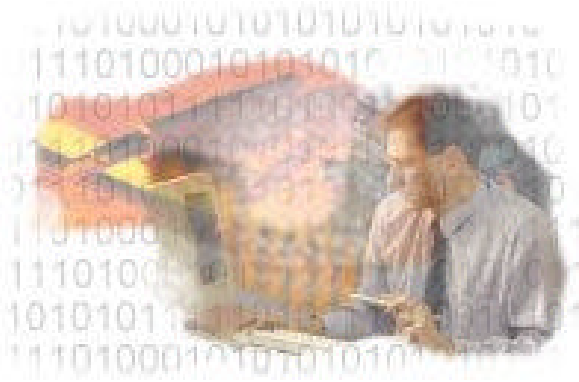
iapo international association of privacy officers

ePrivacy GROUP™

Philadelphia • Los Angeles • London • Washington

Today's Agenda

I. Introduction: Headlines, Paradox & Challenge
II. The Regulatory Landscape
III. Healthcare Privacy and Security
IV. Healthcare Privacy Beyond HIPAA
V. The Role of the Privacy Officer
VI. The Role of the Security Officer
VII. Privacy Trends and Technology
VIII. Lessons from Other Industries
IX. Round Table Discussion



Plus Pop Quiz & Privacy Scenario

I. Introduction

- Privacy/Security Landscape
  - Shaped by laws and lawsuits, regulations, consumer concerns, changes in technology, and above all, human nature
  - Cannot be reduced to a short list of audit and compliance items
- Privacy Paradox
  - Desire to be treated and respect as a person
  - Reluctance to reveal personal information
- Security Challenge
  - To protect information while sharing it.

You Don’t Need Headlines Like These

- Security breach: Hacker gets medical records
  - A computer break-in at the **University of Washington** puts the spotlight on the privacy of medical records -- January 29, 2001
- Eli Lilly Settles FTC Security Breach Charges
  - Federal Trade Commission has settled its case with **Eli Lilly & Co**, the drug giant that inadvertently disclosed the personal information of 669 Prozac users to the public -- January 18, 2002
- Medical Records Security Breach
  - A disturbing security breach at **St. Joseph's Mercy Hospital** in Pontiac, Michigan, left some confidential patient records accessible to the public because the system did not require users to input a password or any other security roadblock -- September 23, 1999

Hard to Claim You Weren't Aware of This...

Stand By Your Privacy Officer?

- Legendary country singer Tammy Wynette was admitted to Pittsburgh University Medical Center under an assumed name (1996)
- Her medical records were sold to paper [allegedly]
- Wynette sued for privacy invasion and paper settled
- What did it cost in terms of reputation, jobs, legal fees, etc?

All of These Could Have Been Prevented

- Database created by the state of Maryland in 1993 to keep the medical records of all its residents for cost containment purposes was used by state employees to sell confidential information on Medicaid recipients to health maintenance organizations (HMOs), and was accessed by a banker who employed the information to call in the loans of customers who he discovered had cancer.
- A medical student in Colorado sold the medical records of patients to malpractice lawyers (1997)
- A convicted child rapist working at a hospital in Newton, Massachusetts, used a former employee's computer password to access nearly 1,000 patient files to make obscene phone calls to young girls (1995)

And All Are Actionable

- The 13-year-old daughter of a Jacksonville, Florida, hospital clerk allegedly used a computer at the hospital to print out a list of patients and telephone numbers. She then called several patients and told them that they were infected with HIV. In one case, she also told a female patient that she had had a positive pregnancy test; that patient attempted suicide.
- A study in five Pittsburgh hospitals found that doctors routinely discuss confidential patient information in elevators, even when other people are present (1995).
- In the not too distant future, incidents like these will be punishable offences under HIPAA,
  - But they are also actionable right now
  - And at no time are they acceptable

What Would The Reaction Be Today?

- 1996: Florida state health department worker used a list of 4,000 HIV positive people to screen dates. List was forwarded to two newspapers (note: this was not a junior clerk but a veteran HRS employee with three masters degrees)
- “Chicago hospital will pay fines of $161,000 resulting from claims of unauthorized duplication of software. The hospital apparently did not have an effective information security program for the protection of proprietary software.” 1997
- Physicians at Harvard Community Health Plan routinely put psychiatric notes into computerized medical records, which were accessible to many of the HMO's employees. 1995

Security Challenge and Privacy Paradox

- **Security Challenge**: Organizations must respect and protect privacy wishes of individuals, but security is accustomed to serving the organization, protecting its secrets
- E.g. when we studied security risks for a large health care company in 1996, security was 100% organizationally focuses, protecting money, assets
- But a personal privacy breach can cost far more than any other form of security breach
- **Privacy Paradox**: People want personal attention but are reluctant to share personal data

The Privacy Paradox

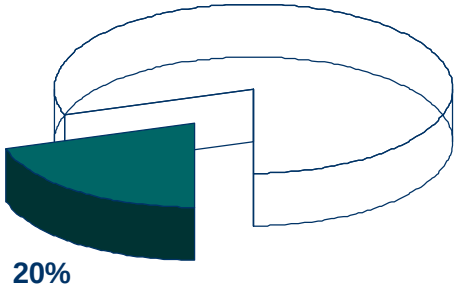
- In many situations, people want a personalized experience
- But they are reluctant to divulge personal information
- In healthcare, professionals need very accurate and very personal information, in order to provide care
- But they may not get it, for a variety of reasons
- Throughout society, any gathering of data today is likely to cause privacy concerns to surface
- A result of adopting information technology faster than we can think about the implications.
- Which means society as a whole still has a lot more questions than answers – which adds to the challenge

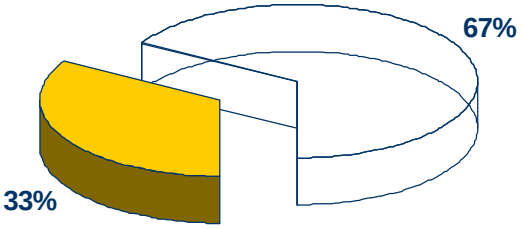
Some Consequences of Privacy Paradox

- People buy less online, people lie more
- People urge politicians to do something
- 67% of consumers had not made two or more purchase in the past six months primarily due to privacy reasons. (IDC)
- 67% of users admit providing false information (Forrester)
- This is a problem for companies AND consumers
- And healthcare is no exception

Example: Healthcare

- One in five American adults believe that a health care provider, insurance plan, government agency, or employer has improperly disclosed personal medical information. Half of these people say it resulted in personal embarrassment or harm.
  - Health Privacy Project 1999, California HealthCare Foundation, national poll, January 1999





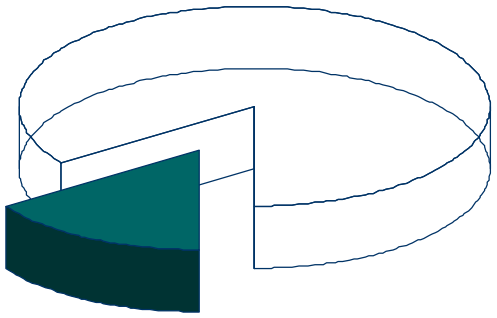
- Only a third of U.S. adults say they trust health plans and government programs to maintain confidentiality all or most of the time.

California HealthCare Foundation, national poll, January 1999

The Fear is Real, With Adverse Effects

- **In a recent survey of Fortune 500 companies, only 38% responded that they do not use or disclose employee health information for employment decisions.**

(Report prepared for Rep. Henry A. Waxman by Minority Staff Special Investigations Division Committee on Government Reform, U.S. House of Representatives April 6, 2000)



15% of American adults say they have done something out of the ordinary to keep medical information confidential.

California HealthCare Foundation, national poll, January 1999

Privacy-protective Behaviors & Effect

- Behaviors
  - Asking a doctor not to write down certain health information or to record a less serious or embarrassing condition
  - Giving inaccurate or incomplete information
  - Paying out-of-pocket
  - Doctor-hopping
  - Avoiding care altogether

- Effects
  - Patient risks undetected and untreated conditions;
  - Doctor's ability to diagnose and treat patients is jeopardized without access to complete and accurate information; and
  - Future treatment may be compromised if the doctor misrepresents patient information so as to encourage disclosure.

So What is Personal Information?

- According to the Federal Trade Commission (FTC), any of the following:
  - Full name
  - Physical address
  - E-mail address
  - Social Security Number
  - Telephone number
  - A screen name revealing an e-mail address
  - A persistent identifier, such a number held in cookie, which is combined with personal information
  - Any information tied to personal information -- age, gender, hobbies, preferences, etc.

Personally Identifiable Information

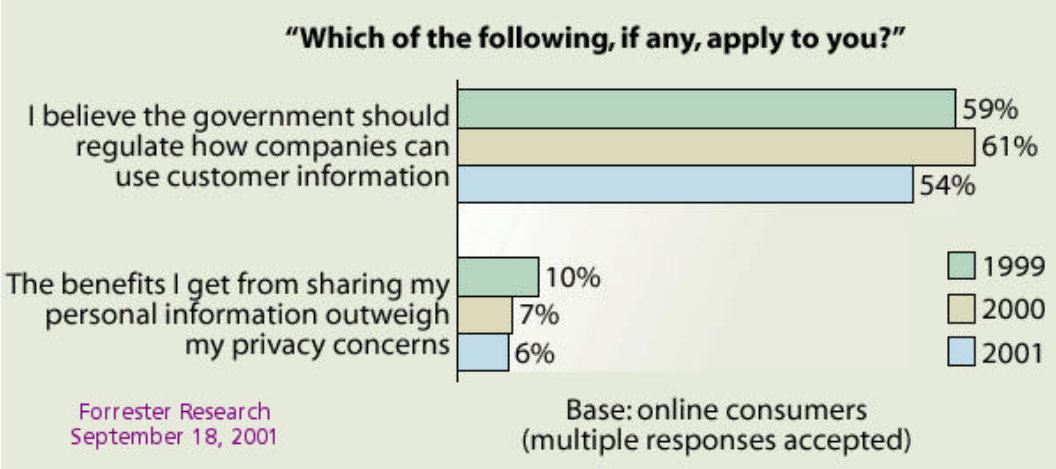
- Information that relates to an individual who can be identified, directly or indirectly, from the data, particularly by reference to an identification number or aspects of his or her physical, mental, economic, cultural, or social identity.

- Which one or two of the following are your greatest concerns over the next century?
  - Loss of privacy 29%
  - Overpopulation 23%
  - Terrorist acts 23%
  - Racial tensions 17%
  - World War 16%
  - Global warming 14%
  - Economic depression 13%

NBC News/ WSJ - Sept. 1999

Privacy Concerns Are Far-Reaching

- Out of a list of eight policy issues, 56% of adults responded that they are “very concerned” about a loss of personal privacy.
- The category came in second out of the eight, beating out such topics as healthcare, crime and taxes.
  - Harris Poll, October 2000
- Healthcare impacts not confined to care, many areas of medical research are also negatively impacted



Privacy Should Be A Concern

- FTC Report to Congress – May 2000
  - Virtually every commercial Web site collects personal information
  - Only 20% implement all four fair information practice principles
    - Notice, Choice, Access and Security
- October 2001 – FTC "Pro-Privacy Agenda"
- December 2001 – FTC "assumes" web privacy policies apply across the enterprise

Recap on Why Privacy Is Important Today

- The issue of privacy could be a decisive factor in the success of the "New Economy"
  - Consumers getting vocal and press coverage spreading (KGAB)
  - U.S. Congress and 50 statehouses are responding with a patchwork of privacy, anti-spam and cybercrime bills
- Organizations of all kinds are struggling with issues
  - Unable to comply or track the evolving multitude of laws, regulations and best practices
- People of all kinds are struggling with issues
  - One reason this is so hard? We don't know what to think (for an example, check out today's privacy scenarios, CO-DMV)
- Consumer trust confidence with respect to privacy are essential for the adoption and use of interactive technologies which fuel may areas of the economy, from pharmacies to disease management

Not Just Our Opinion

- To survive mounting consumer anxiety and the growing labyrinth of US and foreign regulation, firms need to institutionalize their commitment to protecting and managing their customers' privacy by taking a comprehensive, whole-view approach to privacy.
- Anyone today who thinks the privacy issue has peaked is greatly mistaken. As with environmentalism [in the 60s] we are in the early stages of a sweeping change in attitudes that will fuel years of political battles and put once-routine business practices under the microscope.
    - Forrester Report, February 2001

II. The Regulatory Landscape

- There are healthcare specific laws, such as HIPAA and the Common Rule
- But these exist in the context of a wider framework of regulation
- Including
  - State Laws (these are many and varied)
  - Foreign Laws
- Many are based on core tenets of Fair Information Practices (FTC)
  - General & Industry Specific
  - Privacy of Children (COPPA)
  - Privacy of Financial Information (Gramm-Leach-Bliley)
  - Privacy of Medical Information (HIPAA)

Framework of Laws

- Tenets of Fair Information Practices, 1973 Health, Education and Welfare report to Congress:
  - Notice: Disclosure of information practices
  - Choice: Opt-in or Opt-out of information practices
  - Access: Reasonable access to profile information
  - Security: Reasonable security for data collected
  - Enforcement/Redress: Must be a way to enforce these and respond to complaints

Over 30 Federal Laws Affect Privacy

- 1. Administrative Procedure Act. (5 U.S.C. §§ 551, 554-558)
- 2. Cable Communications Policy Act (47 U.S.C. § 551)
- 3. Census Confidentiality Statute (13 U.S.C. § 9)
- 4. Children's Online Privacy Protection Act of 1998
  (15 U.S.C. §§ 6501 et seq., 16 C.F.R. § 312)
- 5. Communications Assistance for Law Enforcement (47 U.S.C. § 1001)
- 6. Computer Security Act (40 U.S.C. § 1441)
- 7. Criminal Justice Information Systems (42 U.S.C. § 3789g)
- 8. Customer Proprietary Network Information (47 U.S.C. § 222)
- 9. Driver's Privacy Protection Act (18 U.S.C. § 2721)
- 10. Drug and Alcoholism Abuse Confidentiality Statutes
  (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)
- 11. Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.)
- 12. Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)
- 13. Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)
- 14. Employee Retirement Income Security Act (29 U.S.C. § 1025)
- 15. Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.)
- 16. Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.)
- 17. Fair Credit Billing Act (15 U.S.C. § 1666)

Over 30 Federal Laws Affect Privacy

- 18. Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)
- 19. Fair Debt Collection Practices Act (15 U.S.C. § 1692 et seq.)
- 20. Fair Housing Statute (42 U.S,C. §§ 3604, 3605)
- 21. Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)
- 22. Freedom of Information Act (5 U.S.C. § 552) (FOIA)
- 23. Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 et seq)
- 24. Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 §§262,264: 45 C.F.R. §§ 160-164)
- 25. Health Research Data Statute (42 U.S.C. § 242m)
- 26. Mail Privacy Statute (39 U.S.C. § 3623)
- 27. Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.)
- 28. Privacy Act (5 U.S.C. § 552a)
- 29. Privacy Protection Act (42 U.S.C. § 2000aa)
- 30. Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.)
- 31. Tax Reform Act (26 U.S.C. §§ 6103, 6108, 7609)
- 32. Telephone Consumer Protection Act (47 U.S.C. § 227)
- 33. Video Privacy Protection Act (18 U.S.C. § 2710)
- 34. Wiretap Statutes (18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605)

Gramm-Leach-Bliley

- Title V - Privacy Act, Pub. L. 106-102 includes two subtitles:
  - Subtitle A - Disclosure of Nonpublic Personal Information; and
  - Subtitle B - Fraudulent Access to Financial Information.
- Part of the act which allows companies to cross- sell financial products and services, written to allay fears of excessive sharing of a person's financial data.
- Defines "Financial Institution" very broadly -- any entity that engages in activities that are "financial in nature" and virtually any other "financial" activity that federal regulators may designate.
  - Hospital Payment plans? Credit? Debt Collection? GLB may apply

GLB: Subtitle A – Disclosure of Nonpublic Personal Information

- Each financial institution has an affirmative and continuing obligation to
  - Respect the privacy of its customers;
  - Protect security and confidentiality of customers' nonpublic PI.
- Financial Institution Prohibited from disclosing nonpublic PI to a nonaffiliated 3rd party (either directly, or through an affiliate), unless:
  - Disclosed to the consumer, in a clear and conspicuous manner, that the PI may be disclosed to such 3rd party;
  - Given the consumer an opportunity to direct that the PI not be disclosed; and
  - Described the manner in which the consumer can exercise the nondisclosure option.

GLB: Subtitle B - Fraudulent Access to Financial Information

- Prohibits obtaining (or attempting to obtain) customer information of a financial institution relating to another person by false or fraudulent means.
- Prohibits a person from causing to be disclosed or attempting to cause to be disclosed to any person, customer information of a financial institution relating to another person by false or fraudulent means.
- These prohibitions apply whether the wrongdoer aims the fraud at the financial institution or directly at the customer.

G-L-B for Non-Financial "Financial Institutions"

- Disclosure
  - No disclosure of account number or similar number or code for a credit card, deposit or transaction account to nonaffiliated 3rd parties for use in
    - telemarketing;
    - direct mail marketing; or
    - other marketing through e-mail
- Privacy Policy
  - Determine policies & practices for
    - disclosing nonpublic PI to affiliates & nonaffiliated 3rd parties;
    - disclosing nonpublic PI of former customers;
    - categories of nonpublic PI collected;
    - protecting the confidentiality and security of nonpublic PI.

COPPA

- The Children's Online Privacy Protection Act (COPPA), enacted October 1998, with a requirement that FTC issue and enforce rules.
- The primary goal is to place parents in control over what information is collected from their children online.
- COPPA applies to:
  - Operators of commercial websites and online services directed to children under 13 that collect personal information ("PI") from children,
  - Operators of general audience sites with actual knowledge that they are collecting PI from children under 13.

Under COPPA You Must Do 6 Things

1. Post clear and comprehensive Privacy Policies describing information practices for children;
2. Obtain verifiable parental consent before collecting PI, with limited exceptions (e.g., usually by fax, telemarketing);
3. Give parents choice to consent to the collection of the PI, but not its disclosure to 3rd parties;
4. Provide parents access to their child's personal information to review and/or have it deleted;
5. Give parents the opportunity to prevent further collection or use of the information;
6. Maintain the confidentiality, security, and integrity of information collected.

Note: COPPA prohibits conditioning a child's participation in an online activity on providing more PI than is reasonably necessary to participate in that activity.

State Privacy Laws

- There is a patchwork of state privacy laws – every state has laws affecting privacy in one of more of the following areas:
- Arrest Records
- Bank Records
- Cable TV
- Computer Crime
- Credit
- Criminal Justice
- Gov't Data Banks
- Employment
- Insurance
- Mailing Lists
- Medical
- Polygraphing
- Privacy Statutes
- Privileges
- School Records
- Soc. Security Numbers
- Tax Records
- Tele. Service/Solicit
- Testing
- Wiretaps Medical information
- Anti-spam and UCE laws
  - www.epic.org

E.g. State Health Privacy Laws

- There is a patchwork of state health privacy laws.
- Some laws cover:
  - specific individuals or organizations; or
  - specific medical conditions
- State laws vary widely
- Current debate over whether HIPAA can preempt state laws or vice-versa.

III. Healthcare Privacy & Security

- HIPAA = Health Insurance Portability and Accountability Act, enacted by Congress in 1996
- HIPAA contains an administrative simplification section, wherein Congress mandated the Secretary of the DHHS to publish regulations to standardize health care EDI
  - EDI is Electronic Data Interchange, a technology for sharing data that pre-dates the Internet
  - Improved EDI
    - = more data flowing
    - = more risk to privacy
  - So privacy standards needed, plus
  - Standards for privacy protection = security

HIPAA Parts

- Title I – Insurance Portability
- Title II – Fraud and Abuse/Medical Liability Reform
  - Administrative Simplification
    - Privacy
    - Security
    - EDI (Transactions, Code Sets, Identifiers)

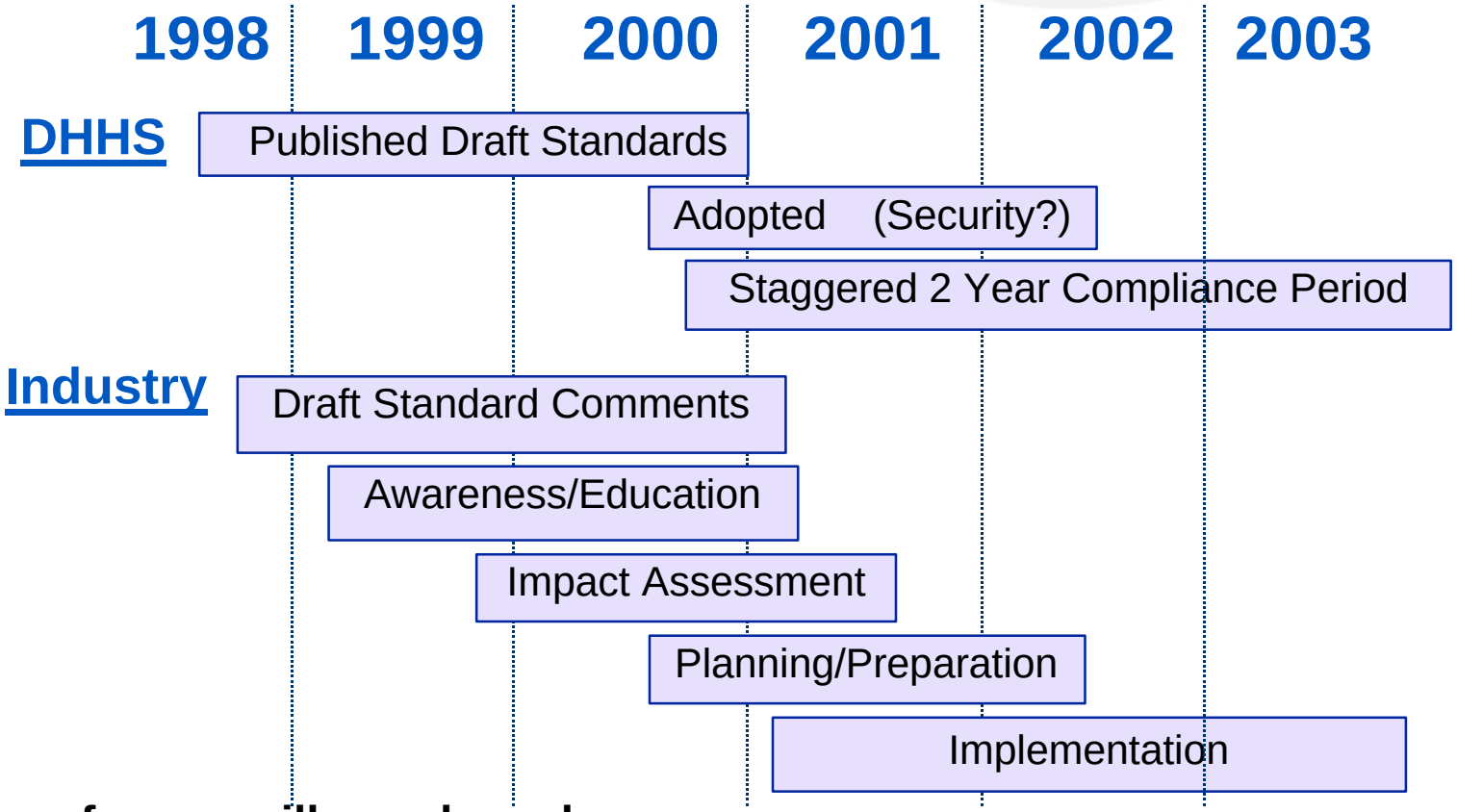
Privacy security officer agenda

- Title IV – Group Health Plan Requirements
- Title III – Tax Related Health Provision
- Title V – Revenue Off-sets

HIPAA Irony?

- Passed in 1996. Gave Congress ample time to draft the privacy and security parts
- But congress declined, so Department of Health and Human Services wrote them and they became law by default
- For the past 8 years, Congress has also failed to pass a patients' bill of rights or a medical privacy act, but
- HIPAA provides elements of both, with little input from Congress

HIPAA Time Line



Time frames will vary based on your organization's particular circumstance

HIPAA Privacy Rule & Covered Entities

- Privacy Rule applies to health plans, health care clearinghouses, and certain health care providers.
- Providers and plans often require assistance with healthcare functions from contractors and other businesses
- Privacy Rule allows providers and plans to give protected health information (PHI) to these "business associates,"
- Such disclosures can only be made if the provider or plan obtains, typically by contract, satisfactory assurances that the business associate will
  - use the information only for purposes for which they were engaged by the covered entity,
  - safeguard the information from misuse,
  - help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them

Covers More Entities Than Expected/Hoped

- Covered Entities:
  - All healthcare organizations. This includes all health care providers, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.
- Business Associates
  - Perform functions involving PHI (PHI may be disclosed to a business associate *only* to help the providers and plans carry out their health care functions - not for independent use by the business associate).
- Hybrid Entities
  - Legal entities that cannot be differentiated into units with their own legal identities yet qualify as a covered entity although covered functions are not its primary functions.

DHHS Timeline

Notices of Proposed Rule Making (NPRMs) Already Published:

Standard	Date of Pub	Final Rule Publication	Compliance Date
Transactions and Code Sets	5/07/1998	Published 8/17/2000	10/16/2002 With exceptions.
National Provider Identifier	5/07/1998	2002	
National Employer Identifier	6/16/1998	2002	
Security	8/12/1998	2002	
Privacy	11/3/1999	Published 12/28/2000	4/14/2003

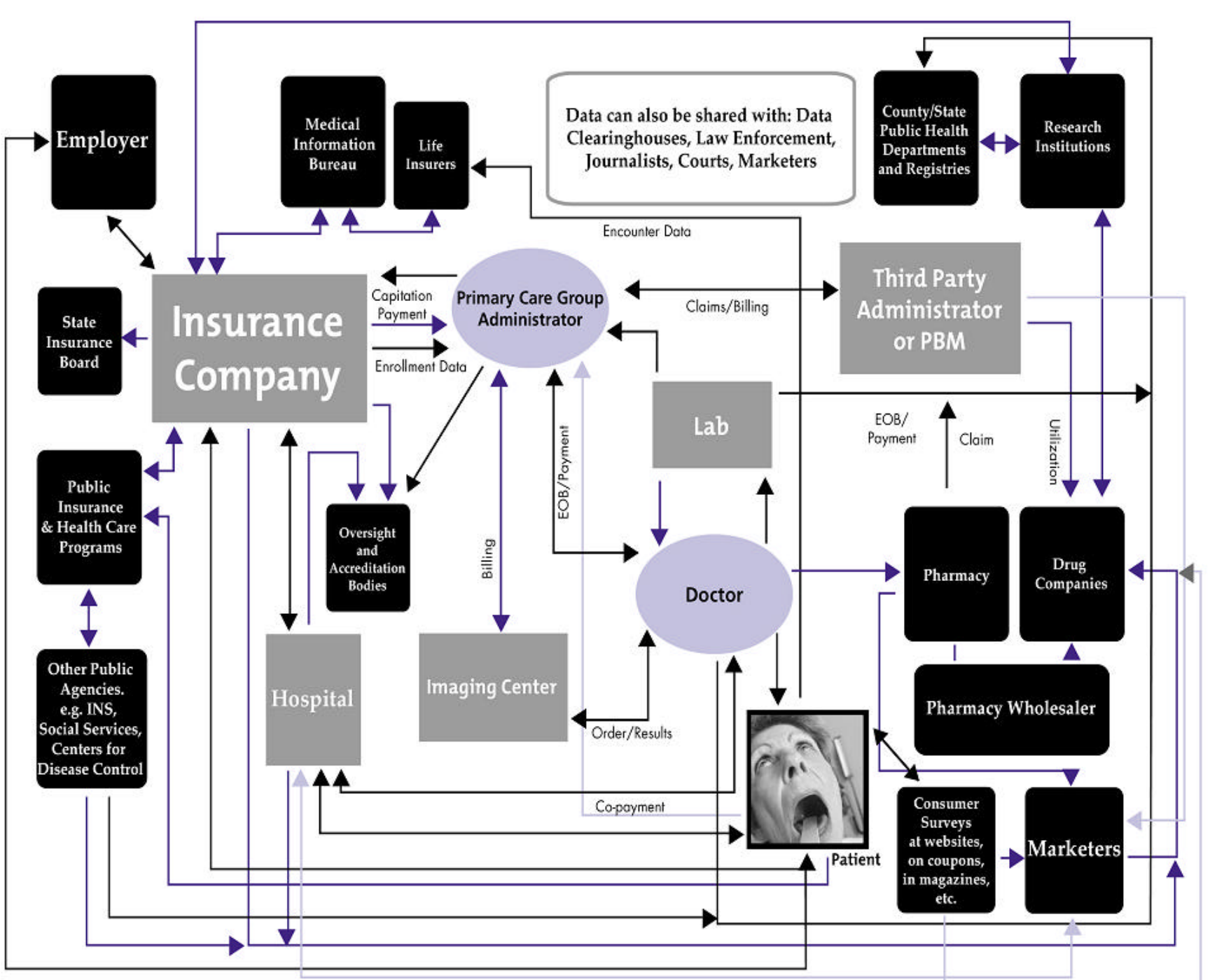
Qualifying for a Delay in Compliance to the Transactions and Code Sets Rule

On December 27th, President Bush signed HR 3323, thereby enabling entities covered by HIPAA to delay compliance with the Transactions and Code Sets Rule by one full year until October 16, 2003. To qualify for the deadline extension, entities must submit a compliance plan to the Secretary of DHHS by October 16, 2002. The plan must include a budget, schedule, work plan, and implementation strategy for achieving compliance. The bill confirms that the compliance date of the Privacy Rule, April 14, 2003, is not affected.

The Clock is Definitely Ticking

- Delays = expense
  - Rush jobs are always more costly (overtime $$$)
  - Experts and vendors will be swamped
  - HIPAA Scope requires complex testing
  - Backlog for implementations likely to cause queues
  - This is an inherently complex undertaking
  - Fine are real and not insignificant (see later)
- Depending upon your place in the healthcare landscape, simply mapping the data flows can be a major undertaking...

Health Care Data Flows



Simplified Health Care Data Flows

As privacy/security officer you will need to know these and map them in detail

Courtesy of
Dr. Ingram-Muhammad
Beacon Partners

So What Does HIPAA Require?

- Standardization of electronic patient health, administrative and financial data
- Unique health identifiers for individuals, employers, health plans and health care providers
- Security standards to protect the confidentiality and integrity of "individually identifiable health information," past, present or future.
- In other words, major changes in the handling of healthcare related information, from the doctor's office to the insurance company, your HR department, the hospital, the janitors and the IS staff.

What Does HIPAA Mean In Terms of Privacy?

- 164.502 Uses and disclosures of protected health information: general rules.
  - (a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.
- 164.530 Administrative requirements.
  - (c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

What Does This Mean?

- Patients will have the right to review and copy their medical records, as well as request amendments and corrections to these records
- Physicians must obtain written permission from patients before information for routine matters such as billing and treatment can be shared with others
- Health care providers and plans must tell patients to whom they are disclosing their information, how it is being used
- IIHI must be protected at all times, disclosed only when necessary, and only as much as necessary

Privacy Aware Practices

- Staff must be trained on what this all means in terms of office procedures, enquiries, transactions, visits, emergencies, etc.
- Compliance documentation will need to be managed
- Covered entities must establish business practices that are "privacy-aware" such as:
  - Training staff about privacy issues
  - Appointing a "privacy officer"
  - Ensuring appropriate safeguards for IIHI

Practical Implications

- Besides the changes in business practices
- Providers and insurance companies must rewrite contracts with business partners such as auditors, attorneys, consultants, even the janitors, to ensure that they adhere to the privacy rules.
- Many unwritten rules must be written down, and some will need to be changed

Your Best Bet?

- Find out if covered, what covered, now
- Begin education now
  - Lack of HIPAA specific privacy training?
  - No problem (common body of knowledge, Fair Information Practice Principles, OECD, etc.)
- Act in spirit of the act and document efforts
- Document all decisions with respect to IIHI
  - Why you handle the way you do
  - Why you protect the way you do

Because HIPAA Has Teeth

- The Act provides severe civil and criminal penalties for noncompliance, including:
  - fines up to $25K for multiple violations of the same standard in a calendar year (e.g. erroneous data)
  - fines up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information
- And other, serious liability implications

Liability Under HIPAA

- Basis of liability
  - Federal statute/regulation
  - State statutes/regulations
  - Internal policies
  - Breaches of agreements
- Liability "activators"
  - Administrative noncompliance
  - Prohibited uses and disclosures
  - Failures to act in accordance with
    - Policies and procedures
    - Agreement terms

Liability Under HIPAA: Who and What

- Enforcement – who
  - Office of Civil Rights (OCR)
  - Department of Justice (DOJ)
  - Attorneys General
  - Private rights of action (?)
- Enforcement – what
  - Agency intervention
    - Informal – voluntary coercion
    - Formal – investigation/audit
  - Civil penalties – OCR
  - Criminal penalties – DOJ
  - State civil and criminal statutes
  - Litigation
    - Remedies
    - Damages

Penalties Under HIPAA

- Penalties
  - **Civil penalties** – $100 per violation up to $25,000 annually for violating the same standard or requirement
  - **Criminal penalties** – Prohibited use/disclosures
    - Knowingly – 1 year and/or $50,000
    - Under false pretenses – 5 years and/or $100,000
    - With malice, for commercial advantage or personal gain – 10 years and/or $250,000

Other Liability

- Complaints
  - Any individual with knowledge
- Litigation
  - Private law suits
    - Affected individuals
    - Other covered entities
    - Business associates
  - Higher standards of care
  - Stricter state requirements

HIPAA Is Also About Healthcare Security

- Paraphrase: “appropriate safeguards to protect the privacy of health information.”
- That is, to ensure *privacy* you need *security*.
- But HIPAA 160 is not specific about security:
  - Implementation specification: safeguards.
  - A covered entity must *reasonably safeguard* protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

HIPAA 142 Gets Specific

- 142 describes “a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure.”
- “we are designating a new, comprehensive standard...which defines the security requirements to be fulfilled to preserve health information confidentiality and privacy as defined in the law.”
  - 45 CFR Part 142, Security & Electronic Signature Standards, Federal Register, Vol. 63, No. 155, 8/12/98

IV. Healthcare Privacy Beyond HIPAA

- Other government agencies have been aggressive in pursuing privacy violations.
  - FTC pursuing COPPA and G-L-B violators
  - Other agencies may seek to get into the action
- Some States have also been active.
  - Individual states acting alone as well as combined actions among multiple states.
- Given current consumer sentiment on privacy, it is to be expected that some public officials will “get tough on privacy.”

The Common Rule Governing Research

- Federal Policy for the Protection of Human Subjects
- Research is “a systematic investigation including research development, testing and evaluation designed to develop or contribute to generalizable knowledge.”
- Can include a wide variety of activities including: experiments, observational studies, surveys, and tests designed to contribute to generalizable knowledge.
- Generally not such operational activities as: medical care, quality assurance, quality improvement, certain aspects of public health practice such as routine outbreak investigations and disease monitoring, program evaluation, fiscal or program audits, journalism, history, biography, philosophy, "fact-finding" inquiries such as criminal, civil and congressional investigations, intelligence gathering.

But Not Common Interpretation

- The Department of Health and Human Services (HHS) regulations [45 CFR part 46] apply to research involving human subjects conducted by the HHS or funded in whole or in part by the HHS.
- The Food and Drug Administration (FDA) regulations [21 CFR parts 50 and 56] apply to research involving products regulated by the FDA.
- Federal support is not necessary for the FDA regulations to be applicable. When research involving products regulated by the FDA is funded, supported or conducted by FDA and/or HHS, both the HHS and FDA regulations apply.
- FDA has not said much about how HIPAA may affect confidentiality of subjects of research

Common Rule, HIPAA, and IRBs

- A covered entity (under HIPAA) may use or disclose PHI for research without an authorization if it obtains a valid waiver approved by an Institutional Review Board ("IRB") or a Privacy Board.
- Otherwise HIPAA requires a covered entity that creates PHI for the purpose of research that includes treatment of individuals to obtain an authorization for the use or disclosure of such information.
- HIPAA's requirements for authorization and the Common Rule's requirements for informed consent are distinct.
- Under HIPAA, a patient's authorization will be used for the use and disclosure of PHI for research purposes.
- In contrast, an individual's informed consent as required by the Common Rule and FDA's human subjects regulations is consent to participate in the research study as a whole, not merely consent for the research use or disclosure of PHI.
- Where all of these rules and regulations are applicable, each of the applicable regulations will need to be followed.

Healthcare Privacy and the FTC

- Aggressive privacy stance – non-healthcare examples:
- Gramm-Leach-Bliley
  - Washington, April 18, 2001Three brokers caught by an FTC sting operation have been charged with violating privacy provisions in the Gramm-Leach-Bliley Act. That 1999 law made it a crime to use deception to obtain and resell bank account balances, information on stock portfolios and other financial records.
- COPPA
  - Washington, April 20, 2001: As part of a crackdown on Internet sites that collect personal information from children without their parents' permission, the Federal Trade Commission announced yesterday that three online companies have agreed to pay $100,000 in fines to settle charges that they violated federal law.

FTC Non-Health (But Relevant) Examples

- Geocities (Aug 2000)
  - Violation of promise not to share personal information with third parties
    - Geocities Stated that without permission, it wouldn't release information about a person's education, income, marital status, occupation and personal interest
    - Sold that information to advertisers
- Liberty Financial Companies (May 1999)
  - False claim that personal information maintained anonymously
    - "Young Investor" site (www.younginvestor.com)
    - Directed to children and teens, and focuses on issues relating to money and investing.
    - Personal information about the child and the family's finances was maintained in an identifiable manner.

More FTC Examples – Medical Security

- Toysmart.com (July 2000)
  - Sale of customer list in bankruptcy contrary to privacy policy
    - Sale of data as separate asset forbidden
    - COPPA related incident
- Sandra L. Rennert and Medical Group, Inc. (July 2000)
  - Misrepresenting security measures to protect medical information and how it would be used
    - Improper disclosure of medical information
    - Individual and corporate responsibility

FTC Examples (4 of 4): Eli Lilly Case

- As part of prozac.com, Eli Lilly sent out individual email reminders to 700 people who used their reminder service
- But when Lilly discontinued the service, June 01, the notice was sent to the entire list, using “cc” and not “bcc” and thus revealing addresses of recipients to all
- The ACLU asked FTC to investigate as an “unfair or deceptive trade practice” because customers had been led to believe that their identities would be kept secret.”
- Incident was an “accident” but occurred because of a lack of privacy awareness on part of employees handling the mailing program
- Immediate damage – company banned ALL outbound email with more than one recipient (imagine!)

Lilly FTC Update 1/2

- The proposed FTC settlement would prevent Lilly from making further misrepresentations about the extent to which they maintain and protect the privacy or confidentiality of any personal information collected from or about consumers.
- Lilly would be required to establish and maintain a four-stage information security program
  - designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect consumers' personal information against any reasonably anticipated threats or hazards to its security, confidentiality, or integrity, and to protect such information against unauthorized access, use, or disclosure.

Lilly FTC Update 2/2 (Try Figuring Costs on This!)

- Specifically, Lilly would be required to:
  - designate appropriate personnel to coordinate and oversee the program;
  - identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including any such risks posed by lack of training, and to address these risks in each relevant area of its operations, whether performed by employees or agents, including: (i) management and training of personnel; (ii) information systems for the processing, storage, transmission, or disposal of personal information; and (iii) prevention and response to attacks, intrusions, unauthorized access, or other information systems failures;
  - conduct an annual written review by qualified persons, within ninety (90) days after the date of service of the order and yearly thereafter, which shall monitor and document compliance with the program, evaluate the program's effectiveness, and recommend changes to it; and
  - adjust the program in light of any findings and recommendations resulting from reviews or ongoing monitoring, and in light of any material changes to Lilly's operations that affect the program.

V. The Role of the Privacy Officer

- Roles of the CPO
- The CPO's Top 10 Challenges
- 10 Action Items for the Privacy Officer
- 10 Time-Saving/Cost-Saving Suggestions
- Cost of a Privacy Blowout

"He that prieth into every cloud...
may be struck with a thunderbolt."

- English proverb

Privacy Officer Has Internal/External Roles

- Internal Role
  - Company-wide Strategy
  - Business Development
  - Product Development & Implementation
  - Operations
  - Security & Fraud
  - Corporate Culture
  - Facilitator:
    - with senior management support, forge long-term cross-disciplinary privacy model
    - problem solve for team members
    - assure cross disciplinary training
- External Role
  - Industry Relations
  - Government Relations
  - Media and PR
  - Privacy Community
  - Consumer Relations

The Privacy Officer's Top Ten Challenges

1. Data = corporate "family jewels," but value = use
2. Contractual protections helpful, but not enough
   - breach, leakage
3. Security threats: hackers & the marketing dept.
4. New products/services requiring review of data policies
5. New partnerships/alliances requiring coordination of policies
6. Data "bumps" (combining databases, augmenting data)
7. M&A issues (merging differing policies), Bankruptcy
8. Monitoring for compliance in fast-moving organizations
9. Consumer fears are as high as ever, media enjoys feeding fear
10. Legislators/regulators eager to turn that fear to their advantage

10 Privacy Officer Action Items

- Three areas:
  - "Know what you do."
  - "Say what you do."
  - "Do what you say."

“Know what you do.”

1. Assess your data gathering practices
   - Database Administrator is your friend
   - Division level, department level databases?
   - Business development deals? Marketing plans? (“data bump”)
2. Understand your level of "permission“
   - “Legacy” databases and past practices
   - Past performance v. future expectations
3. Assess your defensive measures against outsiders
   - Network security audits (e.g., TruSecure)
4. Assess your defensive measures against insiders
   - Consider centralized policies if not centralized control
   - Access restrictions

“Say what you do.”

(a/k/a Drafting/Revising your Privacy Policy)

5. Clearly disclose all relevant practices
   - Notice, choice, access, security, redress
6. Plan for changes in practices that are consistent with today’s policy
   - Balancing “weasel wording” with true flexibility
7. If you diverge from today’s policy, *make the changes loud and clear, and move on!*
   - State your case plainly, proudly, and let consumers make their choices

“Do what you say.”

8. Get a Chief Privacy Officer and build a privacy team
   - designate point person in departments
     - Business Development
     - Product Management/Development
     - Operations
   - designate point person for major issues
     - Compliance (regulatory & industry)
     - Legal and Regulatory
9. Implement ongoing security and data audits
10. Integrate privacy into your corporate message
    - Internally (education)
    - Externally (consumer message, industry, regulators)

10 Time-saving/Cost-saving Steps

1. Invest in a good data audit (self or 3rd party).
   - Identifies current practices, uncovers flaws, sets baseline.
2. Invest in a good security audit.
   - Cheaper before trouble occurs v. after trouble occurs
3. Once practices are assessed and problem areas resolved, get certified.* (e.g., TRUSTe, BBBOnline).
   - * know the limitations of certification programs
4. Keep an eye on the political/regulatory scene: AIM, DMA, ITAA, OPA, HHS, FDA, etc.
   - Easiest way to stay ahead of the curve, alerted to data practices that are in media, privacy advocate cross-hairs.
5. No team? Recruit “clueful” staff.

10 Time-saving/Cost-saving Steps

6. Build privacy policies & audit rights into agreements
   - Partners are a weak link; privacy problems spread
7. Don't be shy about bringing in help.
   - Think of auditors, consultants as insurance.
   - When in Rome... get local counsel!
   - Recruit company executives (internal or external) for "Privacy Board" to share responsibility, blame.
8. Plan for disaster.
9. Participate in the legislative process.
   - Prevention is cheaper than cure (ask kids sites).
   - Do us all a favor: if you have a good story, tell it!
10. Join the IAPO: We're all in this together.

Cost of "A Privacy Blowout"

Small.com, Inc. Action	Time (hours)	Cost
• CEO/president time	86	$7,100
• Management time	95	$5,544
• PR meetings and calls	40	$1,067
• Management press calls	26	$1,778
• Management review of privacy practices	15	$833
• Customer service calls and emails	88	$1,944
• Employee communications and training	1	$1,333
• External consultants		$22,500
• Travel		$2,000
Grand total		**$44,099**

BigCompany, Inc. Action	Time (hours)	Cost
• CEO/president time	48	$8,100
• Management time	620	$38,889
• PR meetings and calls	800	$21,333
• Management press calls	76	$5, 456
• Management review of privacy practices	250	$13,889
• Customer service calls and emails	18,750	$416,667
• Employee communications and training	18,770	$335,889
• External consultants		$181,250
• Travel		$16,500
Grand total		**$1,037,973**

Your Privacy Officer Action Plan

- Industry privacy best practices
- What others in your industry are doing about privacy
- Business issues and internal resources
- Helping hands, industry associations, partnerships
- Why it pays to tackle privacy now
- Does your company needs a Chief Privacy Officer?

Act As or Hire a CPO

- Acting as or Hiring a CPO or outsourcing the responsibility is becoming increasingly prudent and necessary to develop privacy policies, oversee privacy efforts and training and to conduct internal audits of business operations.
- CPO is a cross of various expertise
  - Law
  - Security
  - Technology
  - Technology Futurist
  - Domestic & International Politics & PR
  - Marketer

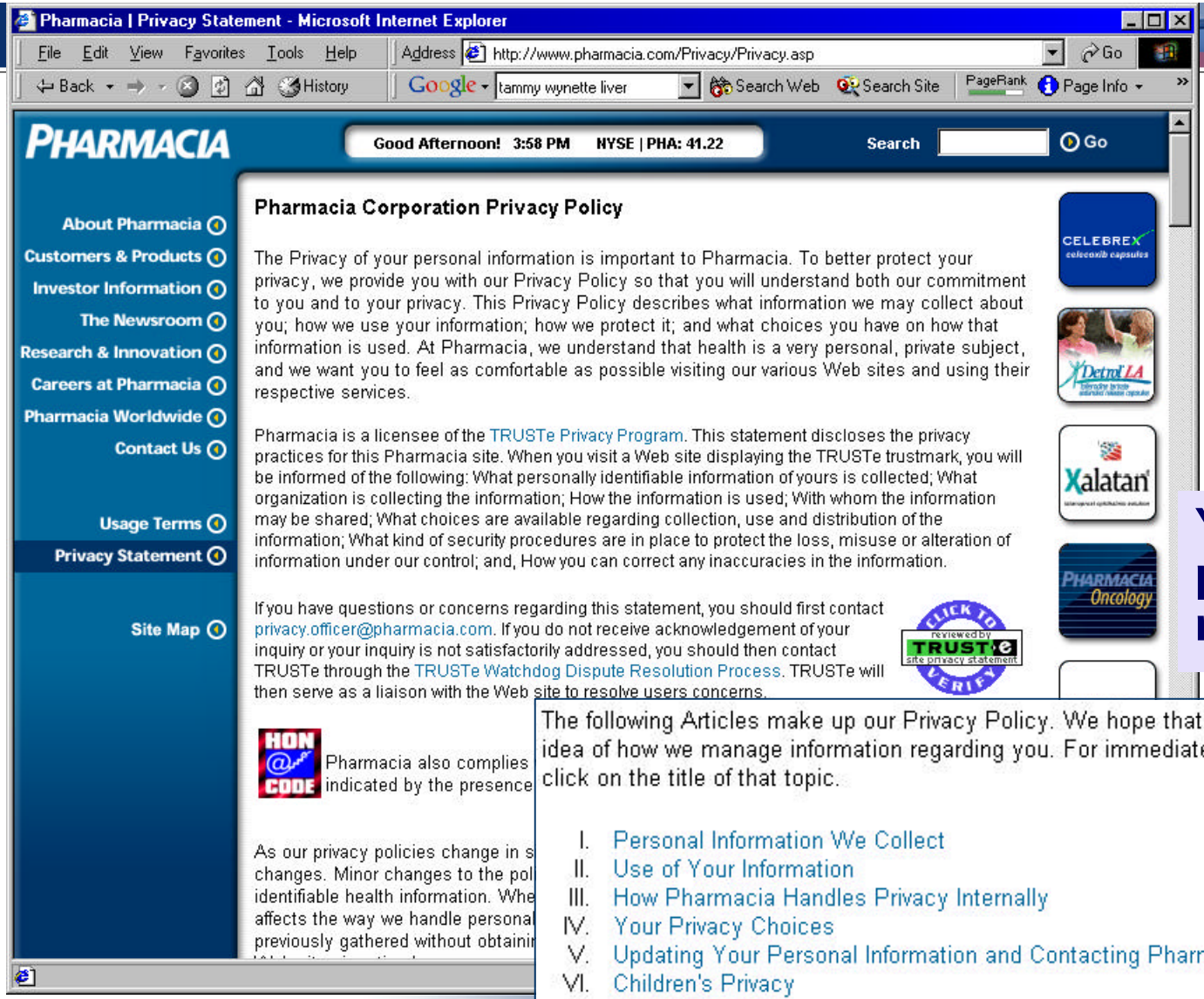
Organization-Wide Privacy Policy

- Develop a privacy policy and privacy practices that are acceptable organization-wide.
- Proactively gain support by corporate counsel and senior management to ensure compliance
- Retain independent expertise to assist in developing, implementing, auditing and reviewing privacy policies and marketing techniques, strategies and technologies.

(Web) Privacy Policy Topics to Review

- What PII do or might you collect?
- Why is or may PII be collected? How will it be used? May online and offline merged?
- Cookies used? Purpose?
- How does one opt-out generally? Onward transfers?
- Do or may you enhance data? How? Why?
- With whom is data shared? Do you co-market? 3rd Parties collect data (e.g., ad servers)
- If you change your policies, how will you let individuals know? Acquisitions?
- Do consumers have access to their PII? How?
- Do you secure PII from unauthorized access?
- Privacy Policy redress?

Web Privacy Policy



Remember, the FTC will hold your organization to this policy

You earn extra points for readability

Harmony in Policy & Practice

- High level privacy principles
- Commitment from the top
- Process to establish and maintain policy
- Broad based education
- Ongoing awareness
- Appropriate process ownership across the enterprise
- Process of checks and balances

Understand Data Flows

- Map data that potentially could come into your company
- Map potential outbound data flows
- Identify where and what is stored?
- Identify major issues
- Identify users and rules of access

Agreements & Contracts

- Review supplier & customer contracts
  - Collect or provide only data needed (not more)
  - Denote the data uses
  - Review terms at renewal
  - Understand supplier's privacy policies and practices

External Messages

- Review all customer touch points, especially sales
- Review marketing literature
- Evaluate Ads & P/R communications
- Identify internal communications that can be shared externally
- Remember that the FTC is looking to prosecute discrepancies between privacy statements and privacy practices
- And the FTC will hold organizations to the highest standard claimed

Training & Awareness

- Privacy and security training pertains to everyone
  - All levels of the organization (whether mandated by compliance with regulations or not)
    - Remember, Eli Lilly case was not HIPAA
- Can be accomplished at low cost per person through technology (web, intranet, video, etc)
- Documented training gives management a “free pass” or at least a strong defense in case of privacy or security breach
  - “We had trained this person, on this date, not to do what was in fact done.”

Training Sample

OBJECTIVE 3RD PARTY ENDORSER **PRIVACY TRAINING**

Demo 1: Introduction to Privacy for Businesses

Page 2 of 9
27 Dec 2001

Privacy is headline news

Over the last twelve months, privacy has rocketed up the public agenda, and consequently, the business agenda, as evidenced by the extensive front page coverage it has received.

A lively public debate about privacy issues was in progress even before the tragic and world-changing events of September 11. Now more than ever, people are thinking about privacy. Companies who care what their customers think are also thinking about privacy, finding out what concerns their customers have and how best to address them.

Extensive media coverage means no company can claim ignorance of current privacy concerns.

ePrivacy GROUP COMPANY LOGO

Home Help Audio Back Next

Compliance Monitoring

- Areas of monitoring should include
  - Policy dissemination
  - Security & IT integrity
  - General compliance and control procedures
  - Disclosure and privacy risk management activities of affiliates and other related parties
  - Internet monitoring of all relevant sites
- Strive for harmony
  - But assume someone will always sing off-key!

VI. The Role of the Security Officer

- Today's Security Officer serves two masters
  - The organization
    - Protecting its data and systems
  - Its customer (patients and others)
    - Ensuring the privacy of their personally identifiable information
  - How did we get here?
- Ensures that systems and data are available for use
- Requires a combination of technical expertise, management ability, and lots of interpersonal skills.
- Increasingly requires knowledge of laws/regulations.

The Difference Between Privacy & Security

- Security is generally about protecting information against unauthorized or unexpected access, while

- Privacy is about defining ownership, content, use and transfer of personally identifiable information.

A Definition of Privacy Protection

- Privacy Protection is the process of
  - guarding the right of individuals, groups and organizations
  - to control or significantly influence the collection, content and use or transfer
  - of personal information about themselves.

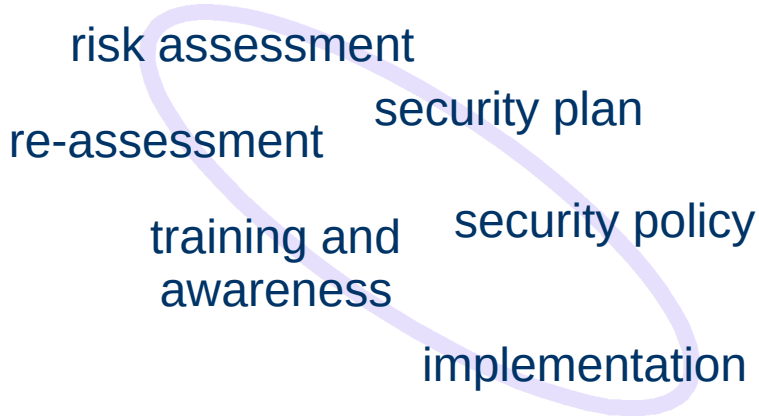
A Definition of Information Security

- Information Security (InfoSec) is the
  - protection of the confidentiality, integrity and availability
  - of information and information assets.
  - Sometimes think of Compromise, Denial & Spoofing

- Technical Definition: The Six Elements of InfoSec
  1. Confidentiality
  2. Control
  3. Integrity
  4. Authenticity
  5. Availability
  6. Utility

Security for the Organization

- Protecting its data and systems, an ongoing task:
  - Risk assessment, security plan, security policy, implementation, training and awareness, assessment
  - Requires top-level endorsement, funding
  - Mid-level cooperation from all departments
  - Training and awareness at all levels



- Plus close attention to all “outsiders”
  - Contracts, connections, suppliers, etc.

Security for Customers (Patients)

- Ensuring the privacy of their personally identifiable information
- Understand their perspective rather than simply implementing legislated requirements
- May need to rein in some departments (e.g. marketing, research, billing)
- But remain focused on the overall goal of the organization, e.g. healthcare delivery
- Customer education can be your biggest weapon for winning customers and defending the organization

While Keeping Systems & Data Available

- Availability is part of security
- You need reliability measures, such as fail over and redundancy (in comms as well as systems)
- Plus incident response plan, in place and tested
  - Who does what when things go wrong
- Plus disaster recovery plan, in place and tested
  - How do you get back your operation capability and system/data availability after things have gone wrong (fire, theft, flood, earthquake, lightning, tornado, etc)

As Part 142 follows Part 160, HIPAA will:

- require each health care entity engaged in electronic maintenance or transmission of health information to:
- assess potential risks and vulnerabilities to the individual health data in its possession in electronic form,
- and develop, implement, and maintain appropriate security measures.
- 142 stresses that these measures must be documented and kept current.

Consider the Implications

- Federally mandated standard for security practices within companies involved in healthcare or handling health-related information.
- Note that these are considered:
  - practices necessary to conduct business electronically in the health care industry today.
- In other words, normal business costs,
  - things you should be doing today, possibly pre-empting arguments over the cost of such standards.

Security practices in the proposed standard

- Organizational Practices
  - Security and confidentiality policies
  - Information security officers
  - Education and training programs, and
  - Sanctions

Use these as a check list for comparison with your current security practices.

- Technical Practices and Procedures
  - Individual authentication of users
  - Access controls
  - Audit trails
  - Physical security
  - Disaster recovery
  - Protection of remote access points
  - Protection of external electronic communications
  - Software discipline, and
  - System assessment.

Physical Security and Data Protection

- Security responsibility must be assigned
- Control of electronic media (access, backup, storage, disposal), including audit trails
- Procedures to limit physical access to systems & facilities (should cover normal operation, as well as “emergency mode” operation and disaster recovery)
- Policy on workstation use
- Secure location for workstations
- Security awareness training for personnel
- Access control, including process for emergency access
  - Either context-based, role-based or user-based access must be provided
- Controls must be auditable
- Data authentication must be provided
- Uniquely-identifiable user authentication, with an automatic logoff feature (PIN, password, token, biometric, or telephone callback authentication must be used)

Data Transmission and Digital Signatures

- Message authentication & integrity controls
  - Either access controls or encryption must also be provided
- If a network is used, the following must be implemented:
  - Alarm capability
  - Audit trails
  - Entity (user) authentication
  - Event reporting
- Use of digital signatures is optional
- If used, digital signature technology must ensure:
  - Message integrity
  - Non-repudiation
  - User authentication

VII. Privacy Trends and Technology

- More laws are coming
- US enforcement of existing laws is increasing
  - FTC under Bush will be aggressive in enforcing current law to forestall pressure for further privacy laws
- Worldwide laws will continue to evolve
  - And many are stricter than US laws
  - Transborder data flows are already affected
  - EU Data Protection Directive
- Privacy Technology
  - The tools to keep data safe on systems already exists
  - More tools will emerge to audit privacy policy and measures
  - More tools will be sold for individual privacy protection
  - Surveillance technology will also increase in power and scope

Privacy Technology Landscape

- Privacy Intermediaries – Trust Them Instead?
  - AOL Screen Name, Cogit, YOUPowered, Microsoft .Net
- Anonymous Browsing
  - Zero Knowledge
  - Anonymizer
  - Tech Specialty Tools
- Anonymous Commerce – Encrypted #
  - Amex, VISA and others
  - Flipping between site for single use
- P3P (Protocol for machine-readable privacy policies)
  - Microsoft led and others support, detailed Privacy protections
  - User manage overall protections and vary for sites they trust

Security Technology Landscape

- Basic tools are well-established:
  - Firewalls, anti-virus, intrusion detection, encryption
- Firewalls now practical for wide range of systems
  - Cheap and relatively easy for SOHO class; larger devices now handle load-balancing, true DMZ architecture
- Anti-virus expanding to include content filtering
  - Protects against system abuse as well as malicious code
- Intrusion detection, systems surveillance
  - Increasingly sophisticated, can be used to monitor internal activity
- You may benefit from steady growth in security skills base
  - But third party audit and verification is still a must

Uneven Security Technology Progress

- Encryption
  - Still lags behind in terms of ease of use and “reliability”
  - Some PKI projects working (note: digital signature not “required” by HIPAA, but guidelines for use)
- Access controls – tokens, smartcards, biometrics
  - Big advances have been made

- New IT developments mean new challenges
  - Handheld devices
    - PDAs, smart phones
  - Wireless devices
    - Infrared, internal 802.11 networks, always on connections

VIII. Lessons From Other Industries

- A reputation for privacy and security can provide a competitive advantage
- 91% of US consumers say they would be more likely to do business with a company that verified its privacy practices with a third party ((Harris, 2002)
  - 62% say third party security verification would allow them to be satisfied with the company
  - 84% think that third party verification should be a requirement
- Peter Cullen, chief privacy officer at Toronto-based Royal Bank, says there's profit in privacy.
  - "It is one of the key drivers of a customer's level of commitment and has a significant contribution to overall demand...privacy plays a measurable part in how customers decide [to] purchase products and services from us. It brings us more share of the customer's wallet."

IX. Roundtable

- Introductions
- Question and Answer Session

Thank You!

Scobb@eprivacygroup.com
Ray@eprivacygroup.com
Mmiora@eprivacygroup.com

Conclusion

Thank You!

Scobb@eprivacygroup.com
Ray@eprivacygroup.com
Mmiora@eprivacygroup.com

Enjoy the Rest of the Conference

Don’t forget evaluation forms...

Notes