Privacy & Security in Medical Research

PRECONFERENCE II

2nd Annual Medical Research Summit

March 24, 2002, 1 p.m. – 5 p.m.

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

iapo international association of privacy officers

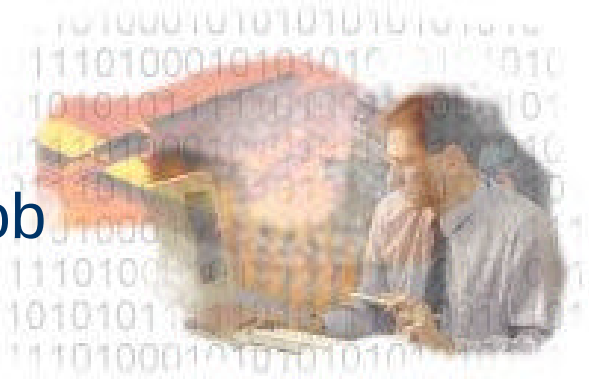
ePrivacy GROUP™

Philadelphia • Los Angeles • London • Washington

www.ePrivacyGroup.com - info@ePrivacyGroup.com - 610.407.0400

Today's Agenda

- I. Introduction – Privacy & Security Headlines
  - These are hot topics (like you hadn't noticed)
- II. In the Name of the Law
  - What laws apply and what do they imply
- III. The "Privacy Proof" Research Program
  - How to make sure both privacy, and your research, are well-protected
- IV. The Security Challenge
- V. The Security Toolset
  - Choosing the right tools for the job
- VI. The Role of the CPO



I. Privacy & Security Headlines

- These are hot topics (like you hadn't noticed)
- 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
  - The Federal Trade Commission has settled its case with Eli Lilly & Co., the Indiana-based 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

Privacy Headlines Fuel Public Concern

There is a Privacy Paradox

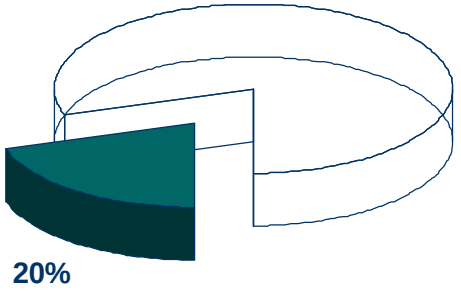
- In many situations, people want a personalized experience
- But they are reluctant to divulge personal information
- In healthcare, professionals need very accurate and very personal information, in order to provide care
- But they may not get it, for a variety of reasons
- Throughout society, any 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

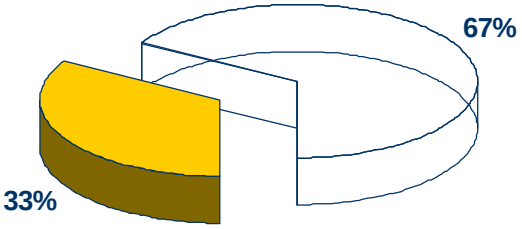
Consequences of the Privacy Paradox

- People may give conflicting answers
  - I want 100% confidentiality for my medical records
  - Yes, you can use my health data for research
- Often not aware of the conflict
  - I don't want anyone but my doctor seeing my health records
  - I do want drug companies to develop better, safer drugs

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





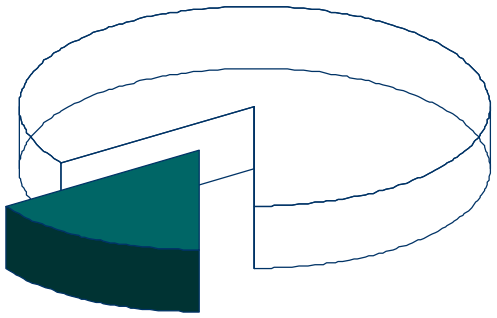
- Only a third of U.S. adults say they trust health plans and government programs to maintain confidentiality all or most of the time.

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 and Private?

- Federal Children's Privacy Protection Act
  - Personal Information includes: a first and last name, a home or other physical address, an e-mail address or other online contact information, including but not limited to an instant messaging user identifier or a screen name that reveals an individual's e-mail address, a telephone number, a social security number, a persistent identifier such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information, or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition.
- European Union
  - Sensitive information includes personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.

State Laws Add Their Own Definitions

- California Consumer Records: Disposal
  - ‘‘Personal information’’ means any information that identifies, relates to,describes, or is capable of being associated with, a particular individual,including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.
- California Identity Theft: Remedies
  - "Personal identifying information" as used in this section, means the name, address, telephone number, driver’s license number, social security number, place of employment, employee identification number, mother’s maiden name, demand deposit account number, savings account number, or credit card number of an individual person.

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.

PIHI, PIMI, PHI, PMI, What's the Difference?

- PIHI: Personally Identifiable Health Information
- PIMI: Personally Identifiable Medical Information
- IIHI: Individually Identifiable Health Information
- PHI: Protected Health Information -- used in a specific context in HIPAA)
- PMI: Personal Medical Information
  - Different from "identifiable"
  - An important distinction, particularly in research, PMI can be turned into something that is not identifiable
- We will try to keep these distinctions in mind

II. In the Name of the Law

- What laws apply and what do they imply
- 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 privacy laws 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 (1/2)

- 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 (2/2)

- 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)

Healthcare Privacy

- Although there is no single “Medical Privacy” law, numerous laws are being used to this end, not just HIPAA (of which MUCH more in a few moments)
- The Federal Trade Commission has used its “deceptive business practices” remit to enforce privacy assurances (e.g. Eli Lilly case, of which MUCH more in one moment).
- 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

Healthcare Privacy and the FTC

- Sandra L. Rennert and Medical Group, Inc. (July 2000) involved:
  - Promoting Viagra and Propecia Prescriptions with false medical claims.
  - Collecting consumers' medical and financial data with false privacy assurances
  - Operators of a group of Online pharmacies touting medical and pharmaceutical facilities they didn't actually have and making privacy and confidentiality assurances they didn't keep
- FTC charged promotional claims were false and violated federal laws.
- Settlement prohibits the deceptive claims; requires disclosures about medical and pharmaceutical relationships; bars the billing of charge cards without consumer authorization; prohibits disclosure of the information collected from consumers without the consumers' authorization; and, requires them to notify consumers of their practices regarding the collection and use of consumers' personal identifying information.

The FTC and Eli Lilly (1/3)

- 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!)

FTC and Eli Lilly (2/3)

- 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 (3/3)

- 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.

The FTC Message

- If your organization cannot show that it has made a good faith effort to make all employees who handle PII aware of the proper way to handle PII
- Then don't expect to get off with just a warning
- If you have a privacy incident
- In this case, the company had done a lot of training, and had a lot of security measures
- But the people who managed the program that sent the "offending" email were not adequately aware of the risk/sensitivity of what they were doing, and there was not enough QA to prevent it going out

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

Example 1 of 50: California

- Constitutional Right of Privacy – As amended in 1972
  - Art. I. Sec. 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness, and privacy.
- Tortious Invasion of Privacy
  - Common Law Right of Action
    - Appropriation of the plaintiff's name or likeness
    - Intrusion upon the plaintiff's physical solitude or seclusion
    - Publicity placing the plaintiff in a false light in the public eye
    - Public disclosure of true embarrassing private facts

California Privacy Bills Signed in 2000

- Consumer Credit Reporting: Medical Information
  - Prohibits a consumer-reporting agency from including medical information in reports provided for insurance purposes.
- Disposal of Personal Information
  - Amended Information Practices Act of 1977
  - Requires businesses to take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information, which is no longer retained by the business…
- Office of Privacy Protection (Department of Consumer Affairs)
  - Shall protect the privacy of individuals; personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy arena.
- Disclosure of Marketing Information by Credit Card Issuers
  - Arias Credit Card Full Disclosure Act of 1986 amended to require the credit card issuer to give consumers an opportunity to opt out annually of having PII shared.

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.

The Common Rule Governing Research

- Federal Policy for the Protection of Human Subjects
- Common Rule (codified for the Department of Health and Human Services (HHS) at Title 45 Code of Federal Regulations Part 46) and/or the Food and Drug Administration's (FDA) human subjects protection regulations,
- Research is defined as “a systematic investigation including research development, testing and evaluation designed to develop or contribute to generalizable knowledge.”

Common Rule Includes/Excludes

- 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.

Not Quite 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.
  - Note: FDA has not said much about how HIPAA may affect confidentiality of subjects of research

And So We Come to the Giant 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)

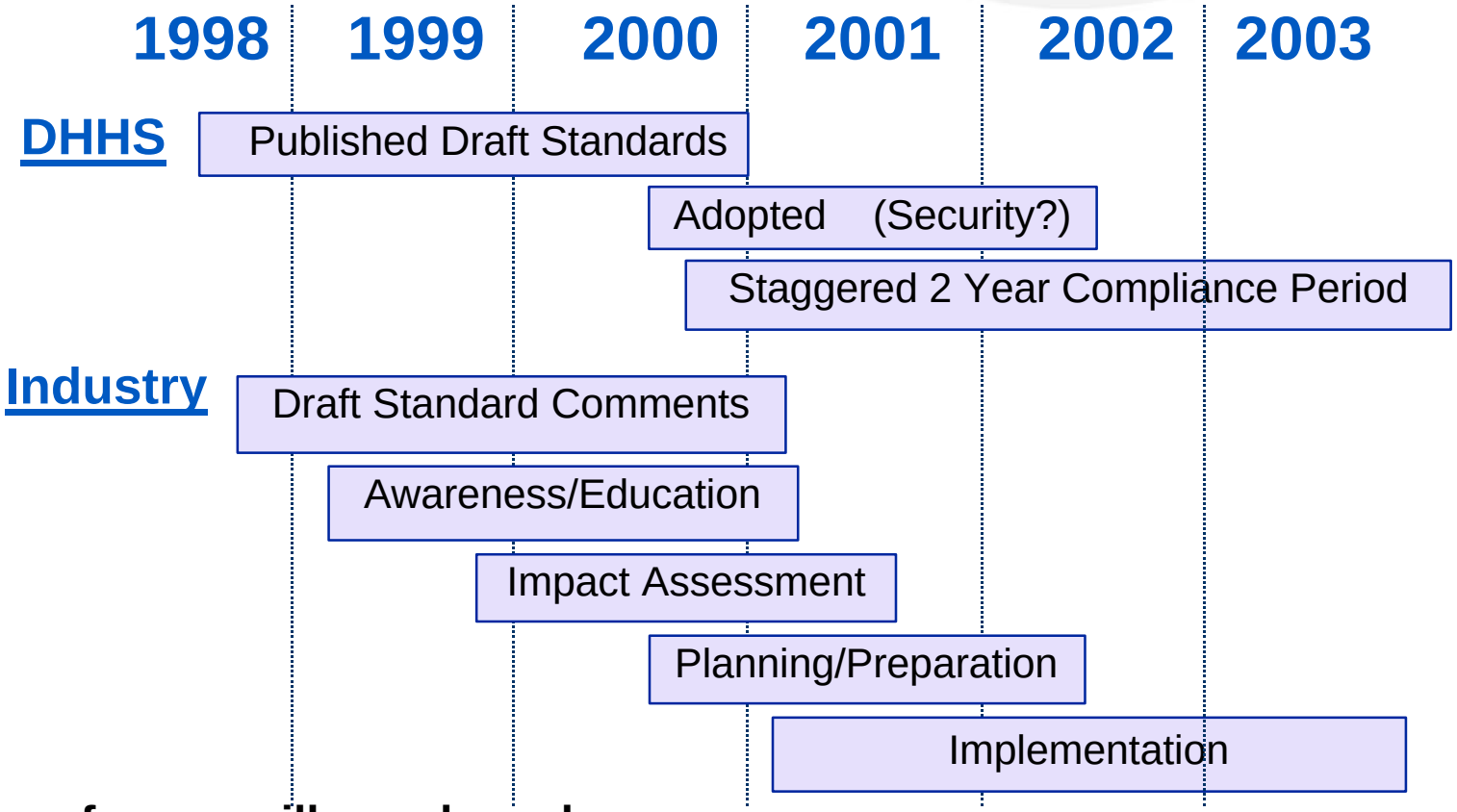
Privacy security officer agenda

- 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.

But Does HIPAA Cover Research?

- The Privacy Rule establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes.
- A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with §§ 164.502(d), 164.514(a)-(c) of the rule)
- The Privacy Rule also defines the means by which individuals/human research subjects are informed of how medical information about themselves will be used or disclosed and their rights with regard to gaining access to information about themselves, when such information is held by covered entities.

DHHS Timeline

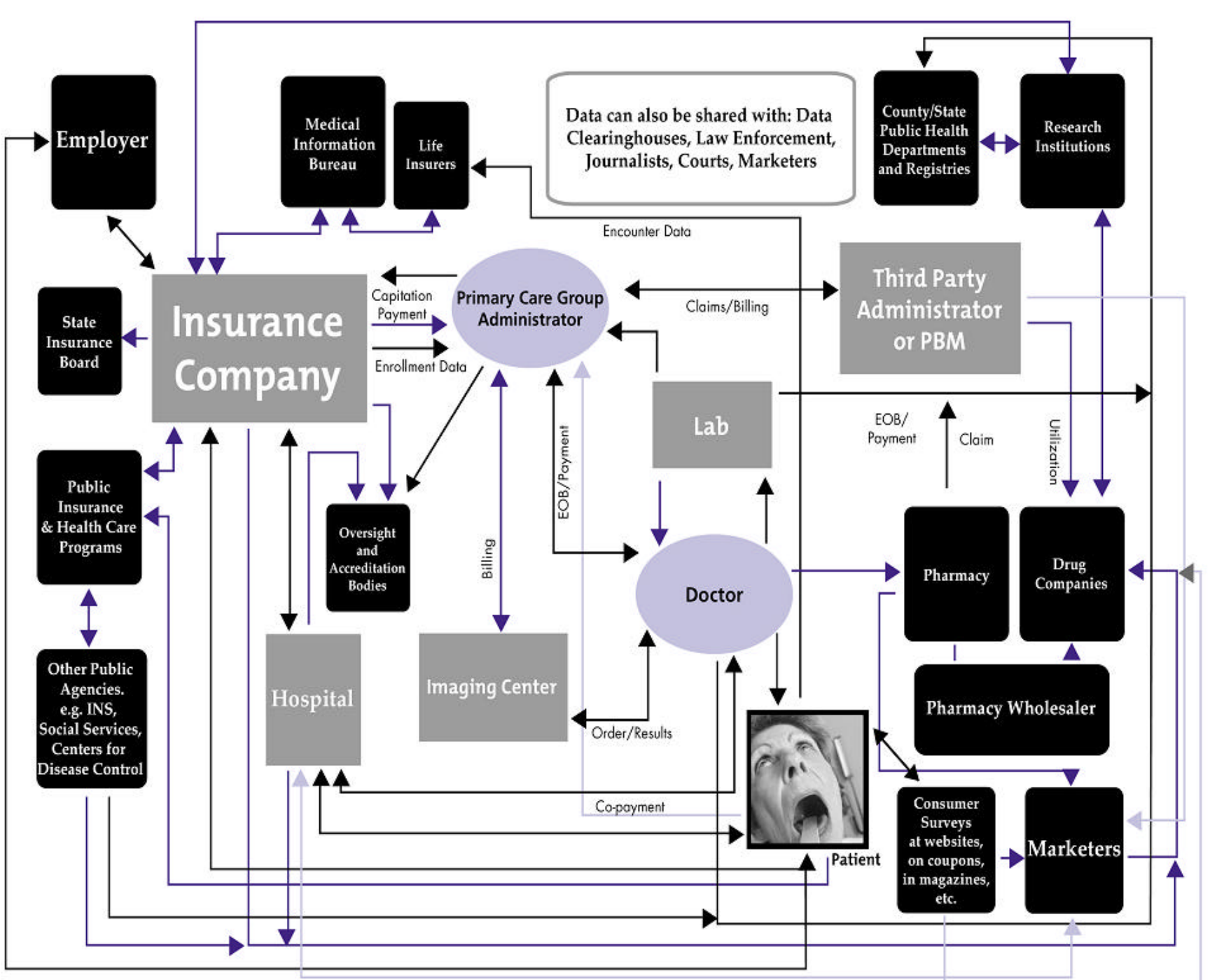
Notices of Proposed Rule Making (NPRMs) Already Published:

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.

Health Care Data Flows



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 Imply?

- 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

Note: 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

Detailed 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 HIPAA-Related Liability

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

III. The "Privacy Proof" Research Program

- How to make sure both privacy, and your research, are well-protected
- The right atmosphere and education
- Knowing what applies
- Documenting your decisions
- Getting the right/best consent applicable
- Maintaining the right level of protection for sensitive data

HIPAA or Not -- Privacy Aware Practices

- Staff must be trained on what privacy means
  - To the goals of the organization and the research effort
  - In terms of office procedures, enquiries, transactions, visits, emergencies, etc.
- Decisions with respect to data will need to be documented and the right documents obtained
- HIPAA 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

Your Best Bet With Respect to HIPAA?

- Find out if covered, then what is covered
- Begin education efforts
- 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

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 v. Common Rule's

- 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.

PHI and Research by Covered Entities

- In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information.
- Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research
  - with individual authorization, or
  - without individual authorization under limited circumstances set forth in the Privacy Rule

Research Use/Disclosure W/o Authorization

- To use or disclose PHI without authorization by the research participant, a covered entity must obtain one of the following:
- Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an Institutional Review Board (IRB) or a Privacy Board (for example, to conduct records research when researchers are unable to use de-identified information and it is not practicable to obtain research participants' authorization).
- Representations from the researcher, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any PHI from the covered entity, and representation that PHI for which access is sought is necessary for the research purpose (for example, to design a research study or to assess the feasibility of conducting a study).
- Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought.

Waiver of Authorization

- A covered entity may use or disclose PHI for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board provided it has obtained documentation of all of the following:
  - A statement that the alteration or waiver of authorization was approved by an IRB or Privacy Board that was composed as stipulated by the Privacy Rule;
  - A statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
  - A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies 8 criteria...(next page)
  - A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board;
  - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as stipulated by the Privacy Rule; and
  - The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

The 8 Criteria

- The use or disclosure of PHI involves no more than minimal risk to the individuals;
- The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
- The research could not practicably be conducted without the alteration or waiver;
- The research could not practicably be conducted without access to and use of the PHI;
- The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
- There is an adequate plan to protect the identifiers from improper use and disclosure;
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
- There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart.

Some Relief?

- De-identified data is not considered PHI
  - Need to thoroughly de-identify
  - May use statistician to certify risk of identifying is low
- Regulatory submission of PHI such as adverse-event data, not affected because Federal agency requires and Privacy Act protects personal data held by Federal government
- Conformance to EU laws on data privacy, since requirements are akin
  - Which brings us to trans-border data flows...

EU Data Protection Directive

- Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995)
- EU Member States must transpose into their national laws
- Covers "personally identifiable data“
- Establishes many principles, on human rights and OECD fair-processing grounds, and procedures

The EU DP Directive

- Restricts "processing“
- Construes "processing" to cover any handling of data
- Applies to all personal data processed in the EU
- Requires that purposes be specified, and that processing be limited to the purposes
- Emphasizes data-subject notice and consent
- Focuses responsibility on “controllers” (who “determine the purposes and means of processing”)
- Protects a variety of data-subject rights
- Requires safeguards and security
- For transfer of personal data to recipients outside the EU, requires “adequate protection”

Putting the Directive into European Laws

- Austria -- DP Act (2000)
- Belgium -- D P Act (1998)
  - Royal Decree on "further processing" (2001)
- Denmark -- DP Act (2000
- Finland -- D P Act (1999)
- France -- in process
  - But 1978 law
- Germany DP Act (2001)
  - six Lander DP laws changed
- Greece -- DP Act (11997)
- Ireland -- in process
- Italy -- DP Act (11996)
- Luxembourg -- in process
- The Netherlands -- DP Act (2000)
- Portugal -- DP Act (1998)
- Spain -- DP Act (1999)
- Sweden -- DP Act (1998)
- United Kingdom -- DP Act (1998)
  - Subsidiary legislation (2000)
  - *Guidance on the Use and Disclosure of Medical Data* (draft)

Principles of Good Data Protection Practice

- The UK Example
- Personal data must be:
  - fairly and lawfully processed
  - processed for limited purposes
  - adequate, relevant and not excessive
  - accurate
  - not kept longer than necessary
  - processed in accordance with the data subject's rights
  - secure
  - not transferred to countries without adequate protection.

U.K. Example: Cascade of controls

- Data Protection Act 1998
- Other laws (Mental Health, Fertilisation, Access to Health Records ...)
- NHS Regulations (Venereal Diseases, Abortion, Genetic Testing
- Professional Guidance
  - British Medical Association, *Confidentiality and Disclosure of Health Information* (1999)
  - General Medical Council, *Confidentiality. Protecting and Providing Information (2000)*
  - Medical Research Council, *Personal Information in Medical Research (2000)*
- Recommendations
  - House of Lords S&T Committee, *Human Genetic Databases: Challenges and Opportunities (2001)*
- New law
  - Health and Social Care Act *(2001)* Section 60 empowers Secretary of State to control processing of NHS and related data
- Draft interpretive guidance
  - U.K. Information Commissioner, *Use and Disclosure of Medical Data* (being revised)

US-EU Safe Harbor Agreement

- Re protection of personal data imported into the U.S. from the EU
- Safe Harbor Principles have to do with:
  - Choice
  - Onward transfer
  - Security
  - Data integrity
  - Access
  - Enforcement
  - Notice

Transfer of data from the EU to the US

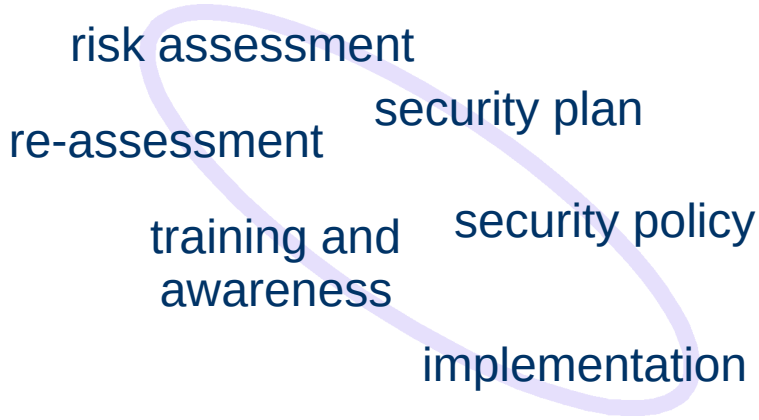
- Assurance option A: Safe Harbor
  - Possible to comply?
  - How cope with the legal imprecision?
- Assurance option B: Data-protection contracts
  - How will contracts be enforced across jurisdictions?
  - EC-endorsed model contract clauses?
- Assurance option C: Self-regulatory code of conduct
  - Who will do this?

IV. The Security Challenge

- Today's Security Officer serves two masters
  - The organization
    - Protecting its data and systems
  - Its customer (patients)
    - Ensuring the privacy of their personally identifiable information
- While also ensuring 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

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/Subjects)

- 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)

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

As 142 follows160, then 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

V. The Security Toolset

- 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

Ongoing Tool Development

- 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

- 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)

Understanding Encryption Basics

- Two types of encryption: private key + public key
- Private key = same password for scrambling and unscrambling (plaintext-ciphertext-plaintext)
- Public key = two keys, one you can share (public), one you keep secret (private)
- The keys are mathematically linked so that:
  - If I use my private key and your public key to encipher a message then only you can decipher
  - Using your private key, my public key
- Key management is the challenge for both types

PKI = Public Key Infrastructure

- Used to enable widespread use of public key encryption
- Employs digital certificates that enable people to find the public key of the recipient
- Note that public key encryption is very computationally intensive, so not used to encrypt the message, just a private key used to bulk encrypt the message
- Private key bulk encryption may be easier for large file transfers between known entities that have secure out of band communication channels

VI. 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/svcs 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?
   - Bus. dev. 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.
   - 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**

Conclusion

- Thank You!
- Scobb@eprivacygroup.com
- Ray@eprivacygroup.com
- Mmiora@eprivacygroup.com

www.eprivacygroup.com/slides

User name: Medres2
Password: Washington