HIPAA Summit IV Preconference III

Basic Privacy and HIPAA Compliance Training for Privacy and Security Officers

Michael D. Bell, Esq.
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
Ray Everett-Church, Esq.
ePrivacy Group
Stephen Cobb, CISSP
ePrivacy Group
Brenton Saunders
PricewaterhouseCoopers
Vincent Schiavone
ePrivacy Group

Sponsored by

iapo
international association of privacy officers

Today's Agenda

I. Introduction – Health Privacy & Security Headlines

II. In the Name of the Law – HIPAA & Beyond

III. Security & HIPAA – For Privacy Officers

IV. HIPAA Compliance Models

Lunch

V. HIPAA Compliance Issues – And the NPRM

VI. Being the Privacy Officer – Some Practical Advice

VII. Health Care Privacy Roundtable

Practical Matters

- There will be coffee breaks
- Mobiles to silent mode please
  - Faculty included
- Remember evaluation forms
  - Leave in place at the end
- The printed handouts
  - Are for Pre-Con III attendees only
  - For additional copies please leave cards marked “slides” or visit web site

- Do not leave valuables in conference room
  - Please perform your own risk assessment as to what constitutes “valuable” in this context (we won’t be offended if you leave your handouts in the room)

I. Health Privacy & Security Headlines

- **August 1996: President Signs New Health Insurance Law**
  - Kennedy-Kassenbaum Bill to Protect Health Insurance for Millions
  - Costs of Health Insurance Portability and Accountability Act (HIPAA) "more than offset" by improvements to computer payment systems
  - New law imposes standards for protection of computerized medical data
- **December, 2000: HIPAA Privacy Rule "Finalized"**
  - By April 14 2003, all "covered entities" must comply with privacy regulations aka "Standards for Privacy of Individually Identifiable Health Information"
  - This Privacy Rule was written by HHS because Congress could not get the job done in the time allowed by the original act
  - Notice of Proposed Rule Making (NPRM) process generated 50,000+ comments which were reviewed before the Final Rule was issued
- **March, 2001: New HIPAA Privacy NPRM from HHS**
  - HHS proposes to modify certain standards in the "Final Rule" with comments due by April 26, 2002 and "final" due by October 13, 2002

Behind the Headlines – The Implications

- The architecture of the new clinic starts to look like this...
- Compliance officers find it harder to find their way around...
- Nobody knows what the “beast” will finally look like, or even when it will appear in its final form...

Behind the Headlines – Seriously

- The fact is, there is nobody here today (or tomorrow or the next day) who can
  - tell you exactly what the Final "Final" Privacy Rule is going to say
  - or give you a guaranteed timeline for the "Final" Privacy Rule

Behind the Headlines – Just the Facts?

- Under such extraordinary circumstances the best you can hope for are “best guesses” and still you may need to read between the lines
- Some people like to think they have the inside track, others espouse a vendor-driven perspective, others have other agendas
- March 14, 2002, Donna Z. Eden, Senior Attorney, Office of General Counsel, HHS, speaking (on tape) to HIPAA Summit West:
  - “I can tell you that the proposed changes are only minor and....the April 2003 deadline is set in stone.”
- Sen. Edward Kennedy, April 16 statement on the proposed changes:
  - “a patient’s nightmare...throws the baby out with the bath water”
- So, if the changes published on March 27 were “minor” then you have to wonder, how solid is that stone?

Behind the Headlines – What Do We Know?

- Ted Kennedy is right about one thing: “The blessing of high technology can also be a curse to personal privacy. With the click of a mouse, our most personal information can be launched into cyber-space for millions to see.”
- Medical data are increasingly computerized, which means, inevitably, medical data are increasingly subject to the risks associated with computer security, namely:
  - Confidentiality: data revealed to people not authorized to see them
  - Integrity: unauthorized changes to data, intentional or otherwise
  - Availability: access to data denied by persons or events
- There is no doubt that the privacy of medical data is at risk
  - Success rate of colleagues testing computer system security and data privacy protections? 100%
  - 100s of tests, over 5 years, often for Fortune 500 companies
  - Average skill level required? 3/5

There Are Plenty of Examples (1/3)

- Medical Records Security Breach
  - A security breach at St. Joseph's Mercy Hospital in Pontiac, Michigan, left some confidential patient records accessible to the public...the system did not require users to input a password, or any other security roadblock. September 23, 1999
- Hacker Gets Medical Records
  - A computer break-in at the University of Washington Medical Center spotlights the privacy of medical records. January 29, 2001
  - Hacker took command of large portions of the Center's internal network and downloaded computerized admissions records for 4,000 heart patients. The medical center was apparently unaware that patient records were downloaded, and elected not to notify law enforcement agencies of the intrusions (which prompted the hacker to go public).

There Are Plenty of Examples (2/3)

- University of Montana Exposes Psychological Records
  - 2001: 400 pages of documents on at least 60 children were posted on the web, in some cases name, address, results of psychological testing, case details. Available to the world for over a week.
- Virginia Teenager Hijacks Doctors' Technology
  - 2000: Virginia teenager impersonated a doctor at the Inova Fairfax Hospital and gave nurses medical orders, including authorizing prescriptions and procedures (such as blood tests and oxygen administration). He forwarded a physician's number to a pager in his possession and returned physician's calls, issued orders.
- HIV List Used for Date Screening
  - 1996: Florida state health worker (a veteran HRS employee with three Masters degrees) used a list of 4,000 HIV positive people to screen "dates." Seen in a bar, list was sent to two newspapers.

There Are Plenty of Examples (3/3)

- Some things don't make headlines, but they happen
  - "Some employees in the emergency rooms of big-city hospitals earn more from passing patient information to ambulance-chasing attorneys than they do from their paychecks," says Columbia University professor Paul D. Clayton, who also runs the information systems at Columbia-Presbyterian Medical Center in New York.
- Consider this example of one doctor's patient notes
  - An MD reads her notes onto tapes, which are then mailed to the transcription agency. An employee there types up the information and emails it back (unencrypted) going to/from the ISP of the person doing the work to a local ISP to which the doctor has an (unencrypted) wireless link. The transcripts arrive as email attachments in Outlook and are saved into Word. She saves a copy onto her hard disk (unencrypted).

And of Course, Plenty of Coverage

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?

Events Like This Erode Patient Confidence

- A 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 HMOs. Same data was accessed by a banker who called in the loans of customers who had cancer.
- A medical student in Colorado was found to be selling 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)

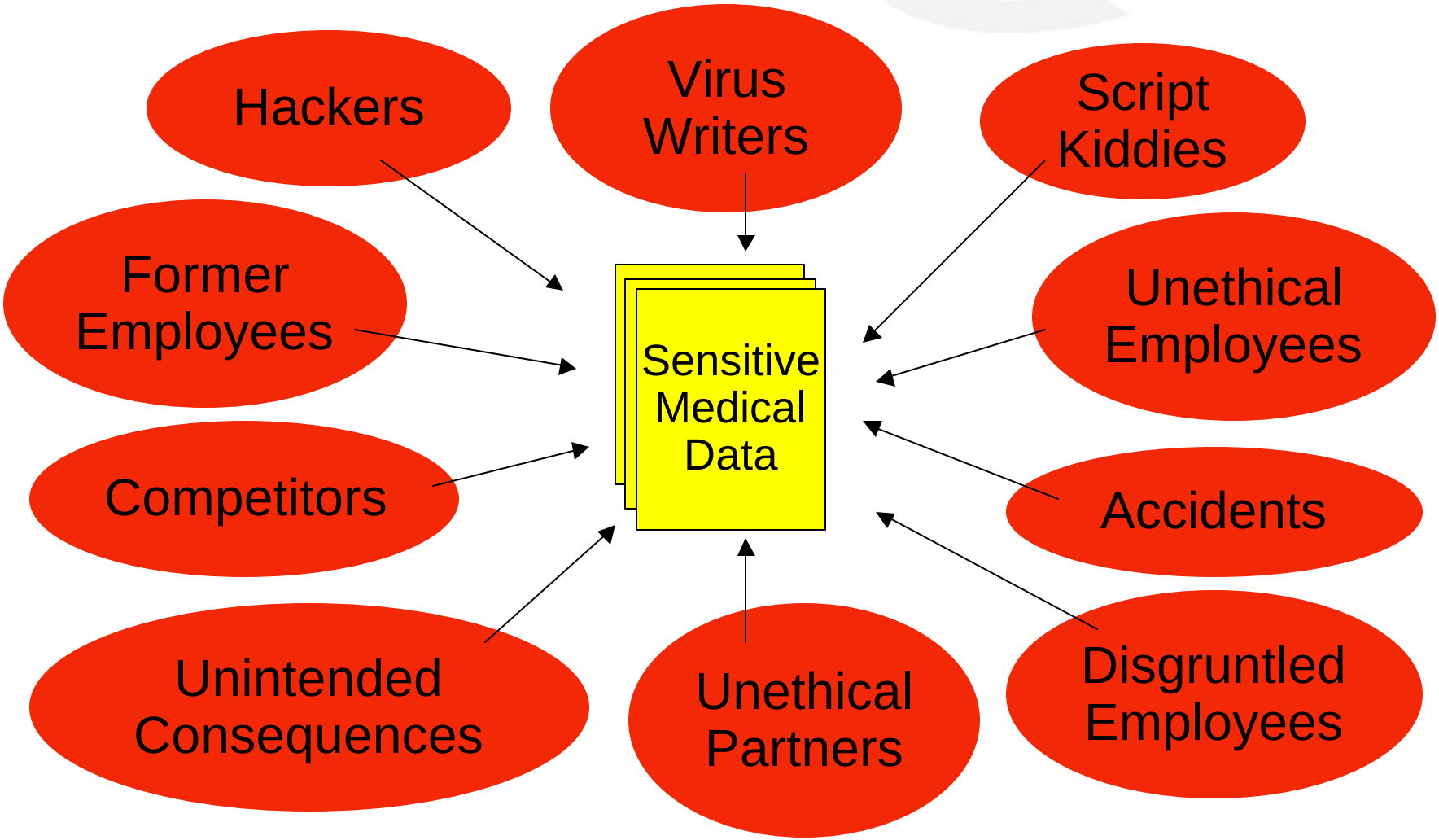
But Why Would Hackers Do This?

- Hackers broke into the computer systems belonging to a clinic in the UK and altered the medical records of 6 patients who had just been screened for cancer -- switched test results from negative to positive, meaning those patients spent several days thinking that they had cancer
- The night before a patient was due to have a brain tumor removed, hackers broke into and corrupted the database where the patient's CAT scans were stored. The surgery had to be postponed while the tests were redone

Why? Because We Can
Slogan from DEF CON III
Las Vegas, 1995

Source: Richard Pethia, manager of the Networked Systems Survivability Program at the Software Engineering Institute (SEI) in Pittsburgh which runs the CERT Coordination Center

Make No Mistake, Your Data is At Risk

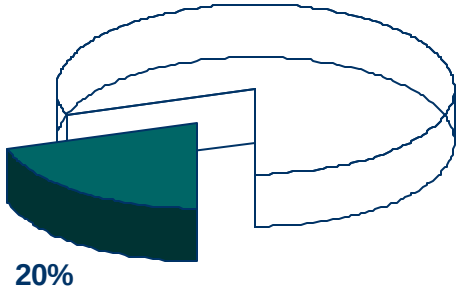


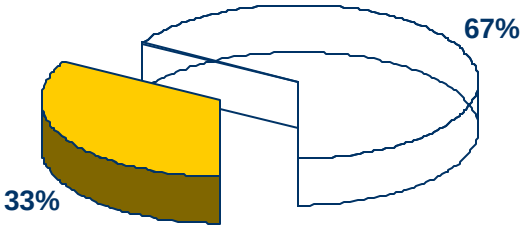
This Is About Privacy and HIPAA

- The Privacy Rule may be changed and the compliance deadline could be delayed
- But privacy concerns are not going away
- For example, if the consent change in the NPRM goes through, a Federally legislated consent requirement could replace it, or states could impose consent requirements
- Regardless of the “final” shape of the HIPAA Privacy Rule,
  - All of these incidents could result in legal action against the institutions involved, right now
  - And of course, at no time are they acceptable

There is a Trust Gap in 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





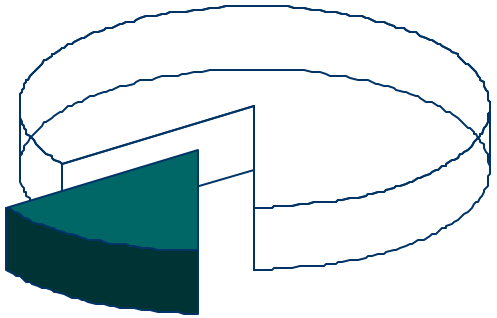
- Only a third of U.S. adults say they trust health plans and government programs to maintain confidentiality all or most of the time.

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.

II. In the Name of the Law

- HIPAA and Beyond
- What laws do Privacy Officers need to know
- Healthcare specific laws
  - E.g. HIPAA, Common Rule, 21 CFR Part 11
- A wider framework of regulation including
  - COPPA, Gramm-Leach-Bliley
  - Federal laws and law (e.g. Federal Trade Commission)
  - State Laws (these are many and varied)
- Many privacy laws are based on core tenets of Fair Information Practices

Framework of Principles Behind 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
- Similar principles found in lots of other places:
  - Organization for Economic Cooperative and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, EU data Directive and US Safe Harbor Principles
  - Include concept of minimum necessary (amount/time/suitability)

30+ Federal Laws on 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)

30+ Federal Laws on 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 Specific Privacy Laws

- Although there is no single “Medical Privacy” law, numerous laws are being used to this end, not just HIPAA
- The Federal Trade Commission has used its “deceptive business practices” remit to enforce privacy assurances (e.g. Eli Lilly case, of which more in one moment).
- Some States have also been active -- individual states acting alone as well as combined actions among multiple states (e.g. Merck-Medco, Minnesota and others)
- Given current consumer sentiment on privacy, it is to be expected that some public officials will “get tough” on privacy, and legislators will want their names on bills
- e.g. the Hollings' Online Personal Privacy Act (HOPPA!*?)

The Point? Privacy Won’t Be Going Away

- Under Hollings' Online Personal Privacy Act, companies which improperly use or disclose sensitive consumer information - or fail to provide adequate access - could be prosecuted by the Federal Trade Commission and the local U.S. attorney's office. In addition, any consumers injured by the company's actions could seek relief in federal court
- Consumer groups say the legal liability provisions are needed as a deterrent against companies that mismanage consumers' personal information - intentionally or otherwise
- Under Hollings' bill, Eli Lilly would have been required to pay at least $3.5 million in damages

The FTC Role: Vigorous Enforcement

- Announced a “Pro-privacy Agenda” last fall
- Has the power to bring action against companies for deceptive practices
- Has already brought action against healthcare companies for privacy violations
- Violations can be based on “deception” if an organization does not deliver on the data protection assurances it makes to the people from whom it collects data (and promises on web sites may be assumed to count for the rest of the organization)

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
- When Lilly discontinued the service, a notice was sent to the entire list, and accidentally revealed addresses of all recipients to each
- 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 blocked ALL outbound email with more than one recipient

FTC and Eli Lilly (2/3)

- The FTC settlement prevents 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 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)

- Company must 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,
- 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 annual written review to document compliance with the program, evaluate effectiveness, recommend changes to; and
- Adjust the program in light of reviews, 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 training, and had security measures in place
- But FTC concluded that the people who managed the program which sent the "offending" email were not adequately aware of the risk/sensitivity of what they were doing, and there was not enough supervision and quality control to prevent it happening

Wait, There's More

- Even without the "cc" snafu this program was a threat
- Messages were sent from prozac.com as email
- Email content is readable unless encrypted and email headers may be readable even if content is encrypted
- Some people had signed up with email addresses that they used/checked at work
- The company network would reveal that they were getting messages from prozac.com
- No spying required – evident in normal network admin operations (and this was not disclosed prior to sign-up)
- Indicates how far ahead of the privacy curve we have moved with technology adoption – clearly corrections are needed if we are going to be serious about privacy

But Is This Relevant?

- Last time we presented these slides, some people said there was “too much about the Lilly case”
- We must assume those people are either:
  - Very confident that SOPs and privacy awareness levels within their organization are so advanced that mistakes like that could never happen there
  - Not personally responsible for protecting the privacy of patient/customer information

State Health Privacy Laws Also Factor

- There is a patchwork of state health privacy laws.
- Some laws cover specific individuals, organizations, medical conditions
- State laws vary widely and we are still working out specific implications of Subpart B - Preemption of State Law
- NPRM reiterates that “the standards, implementation specifications, and requirements established by the Secretary not supersede any contrary State law that imposes more stringent privacy protections”

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 to 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 and 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
  - Credit card disclosure law amended to require the credit card issuer to give consumers an opportunity to opt out annually of having PII shared.

And So We Come to the "Giant" HIPAA

- Health Insurance Portability and Accountability Act
- Enacted by Congress in 1996
- Administrative simplification section mandated the Secretary of the DHHS to publish regulations to standardize health care EDI (Electronic Data Interchange)
  - Improved EDI means cost savings, but also
  - More data flowing
  - More risk to privacy
  - So privacy standards were needed, plus
  - Security standards (for privacy protection)

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 Privacy Rule & Covered Entities

- Privacy Rule applies to health care providers, health plans, health care clearinghouses, health insurers.
- Health care providers and plans often require assistance with healthcare functions from 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

Covered Entities

- Covered Entities:
  - Can include health care providers, health plans, self-ensured 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) Alre

Standard	Date of Pub
Transactions and Code Sets	5/07/1998
National Provider Identifier	5/07/1998
National Employer Identifier	6/16/1998
Security	8/12/1998
Privacy	11/3/1999

Qualifying for a Delay in Compliance to the Transactions and
On December 27th, President Bush signed HR 3323, thereby ena
the Transactions and Code Sets Rule by one full year until Octobe
must submit a compliance plan to the Secretary of DHHS by Octo
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.

NPRM

March 21. HHS Secretary Tommy G. Thompson today proposed changes to health privacy regulations... The proposal would eliminate the need for researchers to use multiple consent forms - one for informed consent to the research and one or more related to information privacy rights. Instead, researchers could use a single combined form to accomplish both purposes. The proposal would also simplify other provisions so that the existing rule more closely follows the requirements of the "Common Rule," which governs federally-funded research. The provisions include privacy-specific criteria and apply equally to publicly and privately funded research...but there is no suggestion that the compliance date of April 14, 2003 will be changed (HHS official recently used the term “Set in Stone”).

So What Does HIPAA Require?

- Standardization of electronic patient health, administrative and financial data
- 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, from the hospital to teaching staff, from the researcher to the pharmaceutical company, from the HR department to the janitors and the IT 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?

- Notice: health care providers with a direct treatment relationship with the patient must obtain consents prior to uses and disclosures of IIHI for treatment, payment, and health care operations (or maybe not).
- Other uses and disclosures will require a specific patient authorization
- Minimum necessary disclosure:
- Access: Patients will have the right to review and copy their medical records, as well as request amendments and corrections to these records
- Security: IIHI must be protected at all times, disclosed only when necessary, and only as much as necessary
- Redress: Fines for non-compliance

HIPAA Definitely Provides Redress (Teeth)

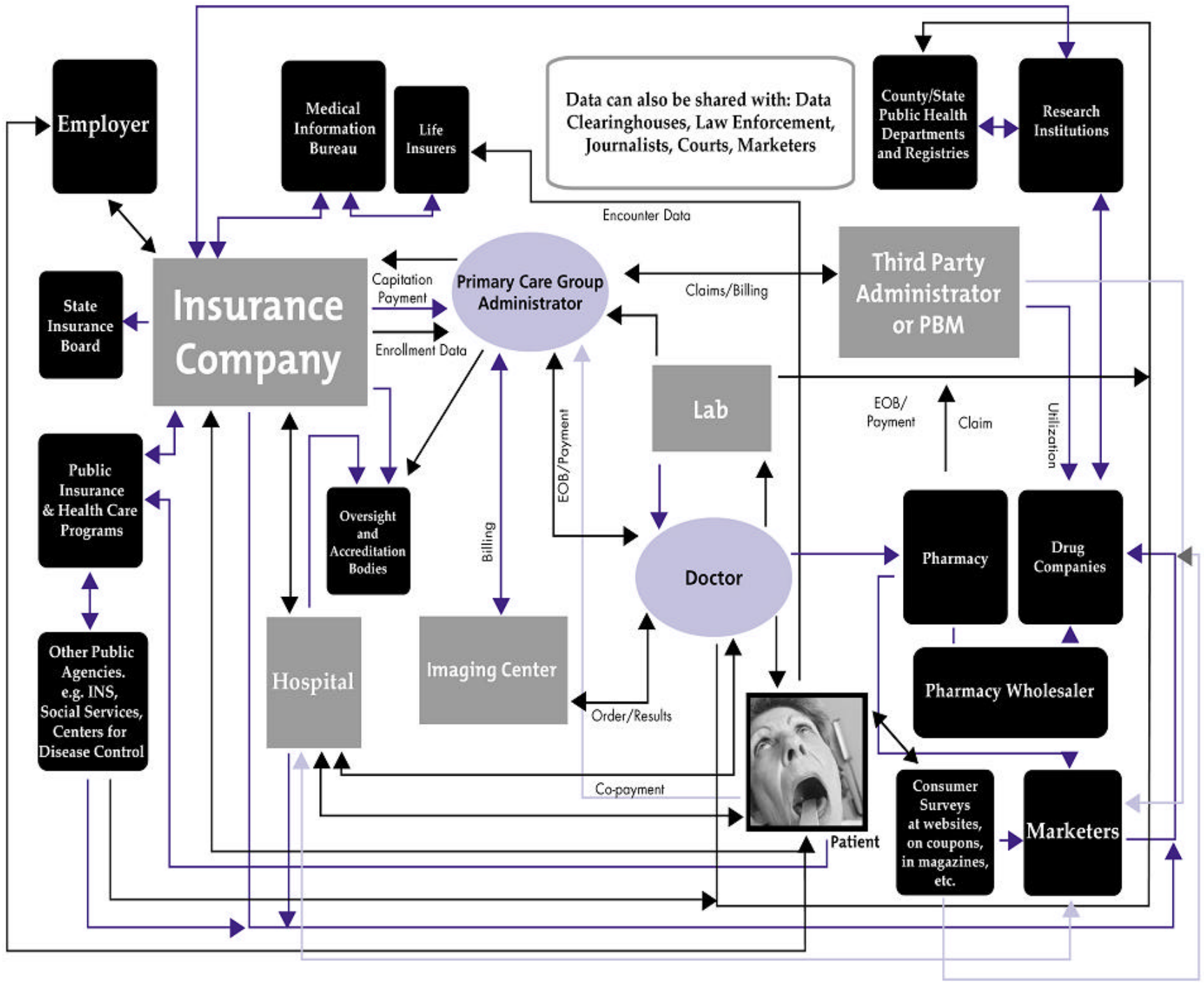
- The Act provides severe civil and criminal penalties for noncompliance, including:
  - fines up to $25K for multiple violations of the same standard in a calendar year (e.g. erroneous data)
  - fines up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health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

Best Bet With Respect to Privacy Rule?

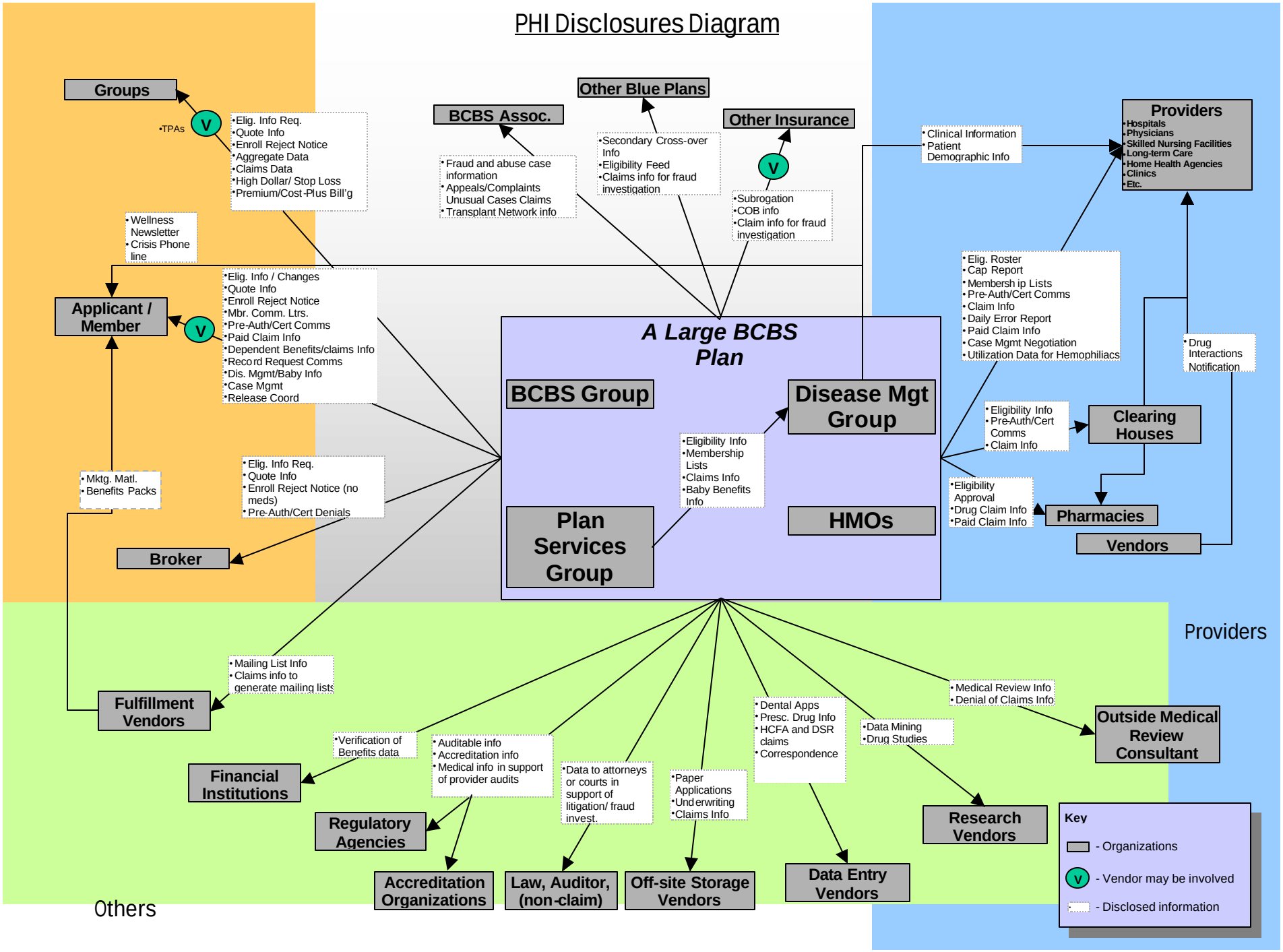
- Map all IIHI flows, know what goes where, and why
- Appoint privacy officer, identify privacy players
- Begin education efforts sooner rather than later
- Act in spirit of the act and document efforts
- Document all decisions with respect to IIHI
  - Why you handle it the way you do
  - Why you protect it the way you do

Compliance Approaches

- Leverage existing compliance programs
- Look at existing infrastructure used to maintain policies and procedures and conduct training
- Conduct an assessment and inventory of current practices.
- Identify the origination, uses, disclosures, and final disposition of the protected health information
- Then you can establish organizational priorities, the work plan


Employer
Medical Information Bureau
Life Insurers
Data can also be shared with: Data Clearinghouses, Law Enforcement, Journalists, Courts, Marketers
County/State Public Health Departments and Registries
Research Institutions
Encounter Data
State Insurance Board
Insurance Company
Capitation Payment
Enrollment Data
Primary Care Group Administrator
Claims/Billing
Third Party Administrator or PBM
Lab
EOB/ Payment
Claim
Utilization
Public Insurance & Health Care Programs
Oversight and Accreditation Bodies
Billing
EOB/Payment
Doctor
Pharmacy
Drug Companies
Other Public Agencies. e.g. INS, Social Services, Centers for Disease Control
Hospital
Imaging Center
Order/Results
Pharmacy Wholesaler
Co-payment
Patient
Consumer Surveys at websites, on coupons, in magazines, etc.
Marketers

PHI Disclosures Diagram



Next Steps

- Identify responsible parties
  - Drawing on existing compliance staff, involving IS, appointing Privacy Officer (required)
- Create a compliance benchmark, gap analysis
  - A snapshot of the organization's current compliance with the requirements of the regulations
- Perform risk analysis and prioritization
  - Identify potential "hot spots" (not required but advisable)
- Assess long-term e-health strategy
  - Extensions or expansions of data flows that are being considered (not required but advisable)
- Line up training resources (in-house, outsource, professional associations)

Tackle Privacy Policies and Procedures

- Update and amend existing policies and procedures to account for the HIPAA privacy and security regulations
- Develop the Notice of Privacy Practices
- Plus specific policies and procedures that evidence compliance with the requirements (currently in flux, e.g. consent and authorization forms)
- Tailor P&P to the functions of each business unit and/or department
- Common element among policies: “minimum necessary”
- Use map of information flow to ascertain all uses and disclosures, and the purposes of such uses and disclosures within each department
- Enable a concise, targeted departmental privacy P&P and informed decision-making with regard to “minimum necessary”

III. Security for HIPAA Privacy Officers

- Security today serves two masters
  - The organization: protecting its data and systems
  - Its customers/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 detailed knowledge of the applicable laws and regulations, like HIPAA security rule, 45 CFR Part 142

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
- While sharing it with appropriate parties
- And making it available to patients on request (in accordance with State and Federal laws and regulations)
- While limiting access to unauthorized persons

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 Mandates 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 follows 160, 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, 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)

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

- Encryption
  - Still lags behind in terms of ease of use and “reliability”
  - Some Public Key Infrastructure projects working
  - Digital signature not “required” by HIPAA

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

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 under HIPAA
- If used, digital signature technology must ensure:
  - Message integrity
  - Non-repudiation
  - User authentication

Your Best Weapon? Training & Awareness

- Security technology without security training is a waste of money (e.g. anti-virus software v. email attachments)
- The single best defense is a security-savvy workforce
- Documented training also creates strong defense for the organization in the event of privacy or security breach
  - "We trained this person not to do that, so we were not negligent"
- Training is required by HIPAA, in security as well as privacy
- And should be done, whether you are covered entity or not
  - Eli Lilly case was not HIPAA and training could have prevented it
- Training can be accomplished at reasonable cost per person through technology (web, intranet, video, etc)

Training Creates Self-Policing Employees

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

3rd Party Training Carries Extra Weight

Thank You!

- Stephen Cobb
- Scobb@eprivacygroup.com
- www.eprivacygroup.com