PRICEWATERHOUSECOOPERS

Getting Through HIPAA Cost-Effectively:
Practical Solutions of 100 Employers

Jon Neiditz
October, 2002

Ingredients of the Most Cost-Effective HIPAA and Privacy Implementation

- Begin with a careful, quick covered entity analysis, drawing clear lines around those areas in which the detailed rules of HIPAA will apply, and those areas in which other privacy policy might apply.
- For most employers, the Benefits area needs to understand the detailed rules of HIPAA privacy, HR needs to understand some relatively basic privacy risk management rules, and IT needs to understand what it needs to change.
- Perform assessment only to the extent necessary to define and accomplish necessary and appropriate projects; you do not need a regulatory audit!
- Never lose sight of what your key business associates are doing or failing to do about HIPAA and offering you (force them to be specific!), and of what other employers are doing about HIPAA.
  - Most employers should not have to build their own systems to perform the privacy administrative functions (or the eligibility/enrollment and premium transactions).
  - Employers will be judged on an emerging consensus about “reasonable” practical solutions for each of the many privacy and security standards.

What is a Group Health Plan?

Covered Benefit Plans

- Medical Benefit Plans
- Long Term Care
- Dental Plans
- Vision Plans
- Prescription Drug Plans
- Many Employee Assistance Programs (EAPs)
- Flexible Spending Accounts
- Personal Health Accounts
- Some Executive Physical Programs

Excluded (though impacted)

- Life Insurance
- Workers' Compensation
- AD&D
- STD and LTD
- Auto Insurance
- Reinsurance/Stop Loss
- Other Property/Casualty

Areas of Employer Risk and Attention

Group health plans:

- change plan documents
- redefine access to and/or use of information within and beyond HR
- redefine access to and/or use of information by labor representatives

Very rarely, provider functions of an employer may be covered, but only if they engage in the standard transactions electronically:

- in-house EAPs
- onsite clinics/pharmacies
- occupational health programs
- other programs providing health services to employees

Review and possible modification of:

- Involvement of local human resources in benefits and other health advocacy
- health and productivity programs
- disease management/ intervention activities
- health promotion/disease prevention
- integrated disability programs
- disability investigations
- individual risk appraisals
- fitness–for–duty exams
- absenteeism studies
- workplace medical and safety surveillance
- union contracts and practices

Examples of Change Driven by HIPAA in Benefits and Human Resources

- Rethinking local HR's involvement in benefits advocacy and health issues
  - Is HR representing the plan, the plan sponsor, the employer as employer or the employee?
  - What levels and types of training does it require?
  - What access, if any, does it continue to have to information from the TPA?
  - If not HIPAA privacy, should broader privacy rules apply?
- The problem of the "coercive" health plan
  - EAPs as a duplicate mental health benefit AND management tool
  - Executive physicals
- Consolidation among TPAs, PBMs, disease management vendors, etc.
  - Can yours get specific about how it will do access, amendment, accounting and alternative addresses on your behalf?
  - Will it indemnify you (meaningfully) for failure to perform those functions or comply with your policies?
- Standard transactions and code sets provide a systems platform on which the number of benefits options can be expanded and options easily removed and added—cutting through delays in responding to demand and transaction costs associated with emerging models in health benefits.
- Do HIPAA privacy and security provide the right backbone of rights to justify the information transfers inherent in consumer-directed healthcare, genomics, e-health, and other trends?

Appendix: Background for Discussion

The Contexts of Privacy Law and Health Privacy

Key Provisions of HIPAA Privacy

- General Requirements
- Special Rules for Group Health Plans
- Firewalls
- Protected Health Information
- Use and Disclosure Rules
- Individual Rights
- Business Associates
- Administrative Requirements

The Context of the Transaction Rules

Major Areas of State Employment Privacy Legislation, 2001-2002*

- 289 bills on background checks and screening
  - 50 have become law
  - Most focus on particular, public-facing professions, including caregiving, law enforcement and school personnel.
  - Many contain employer immunity for releasing information
- 43 on handling of personnel records
  - 17 enacted
  - Including CA and NJ law on disclosure of Workers' comp records
  - CT law requiring that medical records maintained by an employer be retained for 3 years
  - CT and MN law requiring written authorization prior to disclosure of EAP records (CT for public employees only).
  - MN law extending length of time during which involuntarily terminated employees can request reason for termination (to 15 days)
- 30 bills on employee monitoring
  - Only DE's (tit. 19, Sec 7) passed (?), requiring that employers that monitor phone calls, emails or internet access give notice prior to doing so or at the time of hiring, signed by the employee.
  - Many others, including very comprehensive PA bill, made headway.
- 36 bills on genetic testing in employment
  - At least eight passed, all prohibiting discrimination
  - AK and NE regulate use of genetic info, SD prohibits, LA and MD prohibit discrimination, and MN prohibits genetic testing.

*Source: Privacy and American Business May Report

Recent Human Resources Privacy Cases

- Employee computer usage and surveillance of employees each made up 27% of cases monitored*
  - At least one court has held (in Konop v. Hawaiian Airlines) that an employer accessing an employee's website without authorization could constitute an impermissible "interception" of electronic communications under the Electronic Communications Privacy Act (ECPA)
- AMFA v. Northwest Airlines addressed employer limits in background checks
- EEOC v. Burlington Northern: $2.2 million settlement for challenge to workplace genetic testing under the ADA
- Ligand Pharmaceuticals: Class action alleging that Ligand kept the personnel records of a company it acquired in an unsecured place
- Teamsters Local 102 v. Anheuser-Busch: Plaintiff claims hair testing violates employee's privacy rights because it detects drug use up to 90 days before the test, and is discriminatory because the compounds left in the hair by the drugs are more likely to be found in dark or coarse hair…

*Sources: A review by Privacy and American Business of 33 cases through May, 2002

Other Federal and International Law

Other Federal Privacy Law Impacting Employers

- Fair Credit Reporting Act
- Children's Online Privacy Protection Act
- Privacy Act of 1974
- Americans with Disabilities Act
- Gramm-Leach-Bliley Act
- Electronic Communications Privacy Act
- Rapid Development of FTC Interpretations

The E.U. Directive and Other International Privacy Law

- EU Data Protection Directive
- UK Data Protection Act
- Canada – Personal Information and Protection of Electronic Documents Act
- Hong Kong – Personal Data (Privacy) Ordinance
- Australia – Privacy Amendment (Private Sector) Bill 2000
- Japan – The Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector

Privacy: Exposure to Liabilities, Penalties and Reputational Damage

An effort at nationalizing certain privacy standards, HIPAA in fact serves more to **increase awareness, media coverage and enforcement of the complex patchwork of laws, rules and standards, forcing you to get control of your channels through which individual health information flows.**

Penalties

Non-Compliance with Requirements and Standards

- $100 per violation maximum, $25,000 limit per requirement per year
- Penalties for overall non-compliance could reach millions of dollars per year

Wrongful Disclosure of Protected Health information or Misuse of Identifiers (directly or indirectly)

- Simple negligence - $50,000 fine, one year in prison or both
- Disclosure under false pretenses - $100,000 fine, five years in prison or both
- Intent to sell or use information - $250,000 fine, ten years in prison or both

Employers' major exposure likely to be to actions started by whistleblowers

Civil Liability

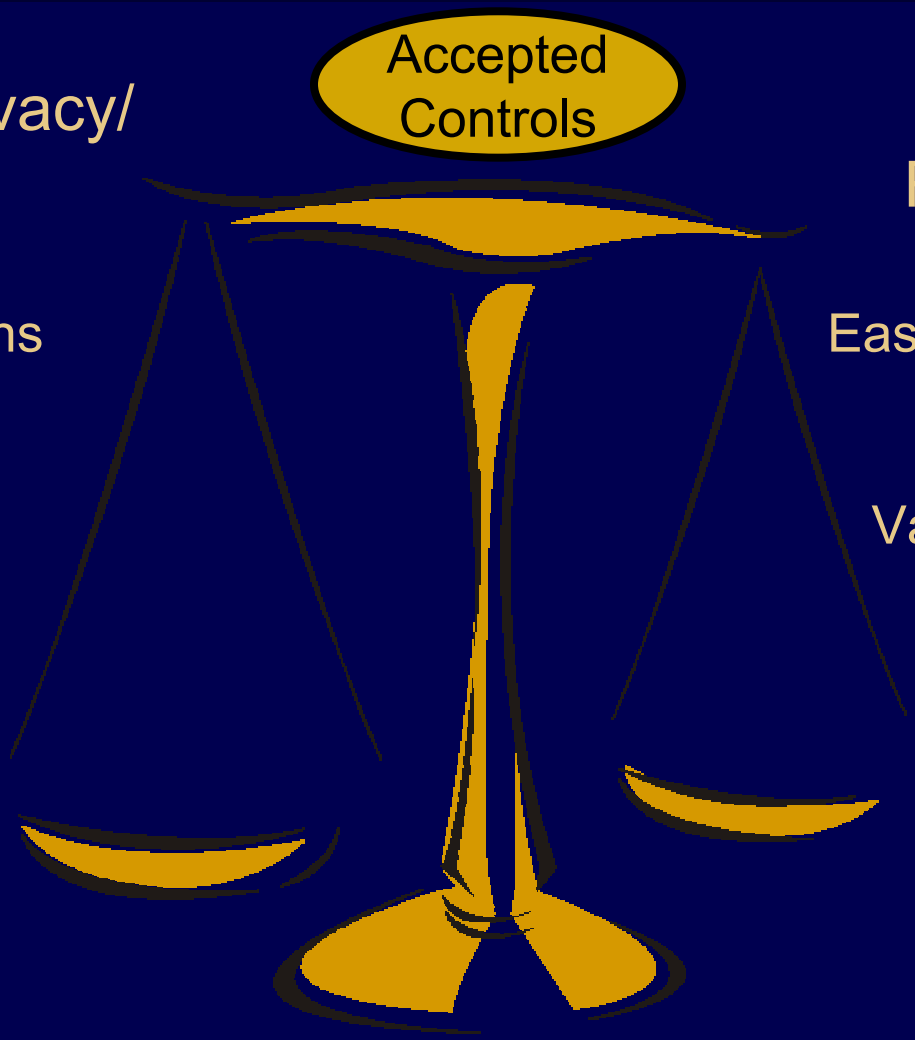
HIPAA privacy and security rules will establish national "standards of care" relating to protection of medical information, for use in state **tort** (e.g., wrongful termination, defamation, negligence and breach of fiduciary duty) suits

New **contractual and consumer protection** theories will be created, based on the terms of HIPAA, Gramm-Leach-Bliley and internet notices, policies, procedures, consents and authorizations.

Balancing Priorities

Information Privacy/
Security Risks

Employee Relations
Media Exposure
Civil Liability
Compliance Risks
Contractual Risks



Business
Requirements

Ease of Administration
Cost Containment
Productivity
Valuable Information
Labor Relations

General Requirements

- **Protecting records** containing individually identifiable health information so that they are not available to those who do not need them.
- **Separating plan administration from other HR functions**, changing plan documents accordingly, and certifying compliance to vendors.
- Providing **information to employees** about their privacy rights and how their information can be used or disclosed.
- Developing and adopting clear **privacy procedures**, and **training** employees on them.
- Designating a **privacy official** to be responsible for seeing that the privacy procedures are adopted and followed.
- Identifying and agreeing to the required contractual provisions with all **business associates**, and taking action if violations become known.
- Establishing processes for **access** to and **amendment** of protected information, and **accounting** for non-exempt disclosures.
- Providing **complaint and remediation** mechanisms and processes.

Special Rules for Group Health Plans

- Generally, the plan sponsor may only receive information from the group health plan or its vendors to carry out "plan administration functions" if it:
  1) modifies its plan documents
  2) places the proper controls on the flow of PHI, and
  3) issues a certification to the group health plan about the protections applied to the information.
- "Plan administration functions" do not include employment–related functions or functions related to other plans.
- Amendments and certifications must:
  - Establish uses and disclosures of PHI by the plan sponsor and its agents, and
  - Ensure adequate separation between group health plan and plan sponsor, in part by describing those employees or groups controlled by the plan sponsor to be given access to PHI, and restricting their access and use.
- If a plan sponsor does not make the required changes in its documents and practices and does not certify that it has done so, it may only receive "summary" information from its vendors, and only in the context of premium bids and of modifying, amending or terminating the plan.

A Privacy Advocate's View of an Employer

HMO/ Insurer

Employer Group Health Plan Function

Plan Sponsor Function

Employer HR/Mgmt Function

Covered Entities

Non–Covered Entities

Protected Information

Protected Health Information (PHI)

- Any information that relates to:
  - Past, present, or future health or condition (physical or mental);
  - Provision of health care; or
  - Past, present, or future payment for the provision of healthcare.
- Which identifies or could be used to identify an individual.
- "CREATED OR RECEIVED BY A COVERED ENTITY OR EMPLOYER."
- Whether in electronic, printed, or spoken form.
- To not be PHI, there must be no reasonable basis to believe that the information can be used to identify an individual.
- For almost all employers' purposes, PHI has the same meaning as Individually Identifiable Health Information (IIHI).

Use and Disclosure of PHI, and the Minimum Necessary Standard

A covered entity may not use or disclose PHI except as permitted or required under the regulation.

- Permitted without obtaining a (very specific, time-limited and freely given) "authorization" from an employee:
  - Payment (e.g., eligibility or coverage determinations, claim adjudication, billing, obtaining reinsurance payments, medical necessity/coverage review)
  - Health care operations (e.g., underwriting, premium rating, etc. for creation, renewal, or replacement of a contract for insurance or benefits, conducting or arranging for medical review, legal services, and auditing functions)
  - Treatment
- Covered entities may use or disclose only the minimum amount of PHI that is reasonably necessary to achieve the purpose of the use or disclosure.
- For routine requests and disclosures, there must be policies and procedures designed to limit the disclosure of PHI to the amount and type reasonably necessary; case–by–case review is not necessary.

New Rights of Employees & Dependents

Individual rights → employer obligations and systems challenges

- Ensure **notification** of privacy rights, policies and procedures (very detailed notice requirements)
- Ensure individuals have **access** to their own PHI (designated record set)
- Allow **amendment** of PHI (designated record set)
  - May deny request but must then allow individual to place an explanation in the record
- Ensure individuals receive an **accounting** of non–exempt disclosures of PHI over the past six years (not limited to designated record set)
  - Excludes treatment, payment, health care operations
- Ensure individuals may request restrictions on use or disclosure of their PHI (though such requests need not be granted)
- Ensure communications are made by an alternative means or at alternative location when requested

Business Associates

Contractors assisting or performing functions for covered entities

Covered entity liable for acts of business associate if it knew of pattern of violations and failed to take reasonable steps (termination, reporting)

Business associate contracts must contain specific provisions:

- permitted uses and disclosures of PHI
- appropriate safeguards of records
- report any unauthorized disclosures
- PHI available for inspection, amendment and accounting
- books and records available for inspection by HHS
- destroy/return PHI at termination of contract
- material breach by associate is grounds for termination

Administrative Requirements

Notice of privacy practices

- Informs participants and beneficiaries of the plan's health information practices, privacy policies, and their rights
- Detailed, specific requirements regarding content
- Must be provided: (1) No later than April 14, 2003; (2) Upon enrollment for new enrollees; (3) Within 60 days of a material revision; (4) Thereafter, every 3 years must provide notice of its availability and how to obtain
- Group health plans:
  - For self-funded benefits, the group health plan must provide the notice
  - For insured benefits, the group health plan may rely on the insurer, but must maintain the notice and provide it upon request
  - If plan provides only insured benefits and receives no PHI, then no requirement to provide or maintain the notice

Administrative Requirements

- Designate privacy official
- Designate contact person and process for privacy complaints
- Conduct privacy training program
- Physical safeguards
- Maintain policies and procedures for protection of health information
- Documentation
- Verification and mitigation
- Refrain from retaliation or intimidation of employees
- Enforce sanctions

Transaction Provisions

Providers	*Challenges for the Self-Administered*	Payors	*Opportunities for Other Employers*	Sponsors
FUNCTIONS		**FUNCTIONS**		**FUNCTIONS**
Eligibility Verification	270 (Eligibility Inquiry) → ← 271 (Eligibility Information)	Enrollment	← 834 (Benefit Enrollment & Maintenance)	Enrollment
Pre–Authorization and Referrals	↔ 278 (Referral Authorization and Certification)	Pre–Certification & Authorization		
Service Billing Claim Submission	→ 148 (First Report of Injury)* → 837 (Claims Submission)	Claims Acceptance	← 270 (Eligibility Inquiry) → 271 (Eligibility Information)	
Claims Status Inquiries	→ 275 (Claims Attachment)* → 276 (Claim Status Inquiry) ← 277 (Claim Status Response)	Claims Adjudication		
Accounts Receivable (AR)	← 835 (HealthCare Claim Payment Advice)	Accounts Payable	→ 811 (Invoice)* ← 820 (Payment Order/RA)	

** Note: These are not contained in the initial Transactions and Code Sets Final Rule*

Your worlds  Our people