PRICEWATERHOUSECOOPERS

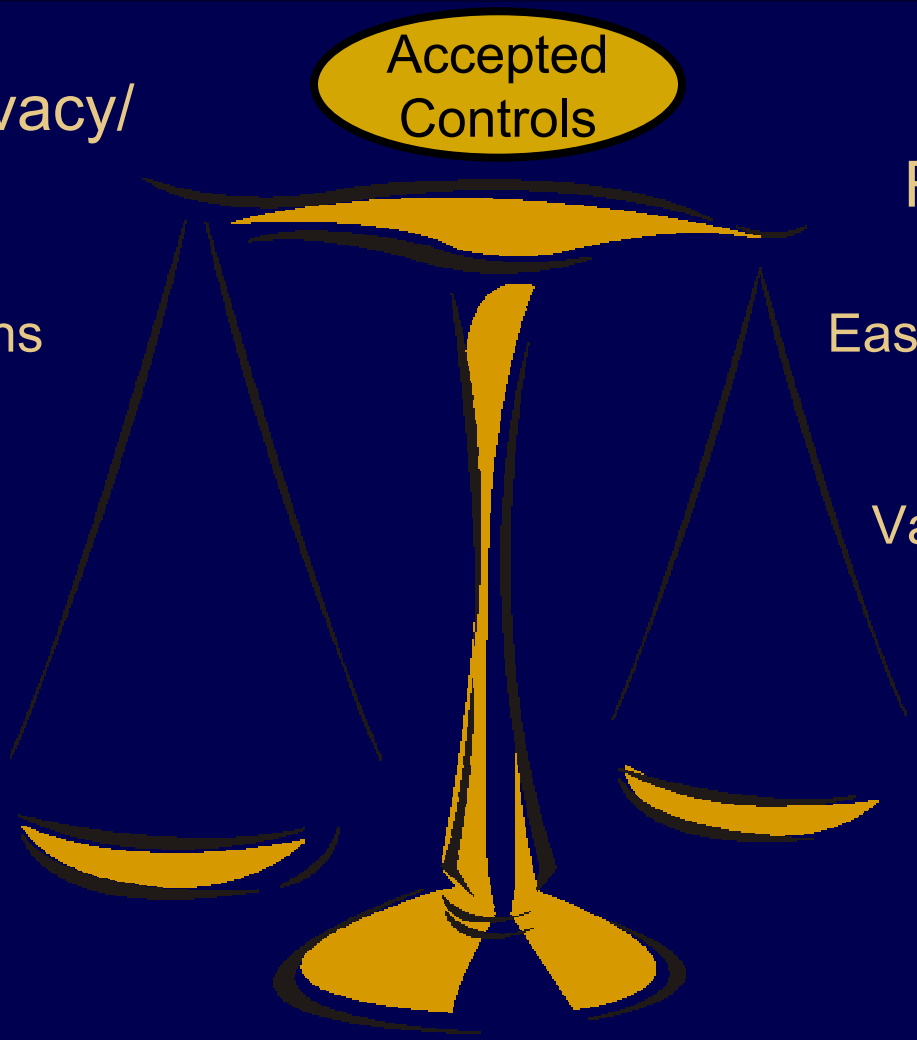
Selected Major Issues in Employer Responses to HIPAA Privacy, at Two Weeks Before the Deadline

Jon Neiditz
March 28, 2003

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

HR & Benefits Advocacy—Introduction

- What is a local HR manager's role when she discusses a health care claim problem with the employee who has the problem?
  - Is she speaking for the group health plan?
  - Is she speaking for the Company as plan sponsor?
  - Is she acting—as always—as a representative of the Company as employer, and as a participant in decisions to promote, discipline or terminate the employee?
  - Is she merely trying to help the employee get the claim paid?
- In almost all the cases in which I've asked the question of HR representatives, the last of these four options has been chosen.
  - However, in no cases I've seen has that role ever been clarified to the employee before.
  - HIPAA requires such a clarification.

Role of HR in Benefits Advocacy 1

- Option 1: Limit HR's role to occasional benefits advocacy, and processing enrollment and eligibility information
  - Keeps HR outside of the firewall between plan administration and employment functions, controlling HIPAA training and compliance costs and HR privacy-related risk
  - The need for "advocate authorizations"
    - The TPAs, the Call Center and/or the Benefits Department won't disclose PHI unless they receive a signed advocate authorization
    - HR is trained on:
      - » the covered plans or components (e.g. medical, prescription drug, dental, vision, long term care, health care spending account, personal health accounts, and perhaps the employee assistance program, executive physical program and/or wellness program) VERSUS
      - » The non-covered programs or components (e.g., short-term and long-term disability, AD&D, workers' compensation, ADA, FMLA, fitness-for-duty exams, drug testing, work-life benefits, leaves of absence, life insurance, auto medical)
    - General HIPAA risk management training ("Do's and Don'ts," scenarios)
    - How are the authorizations and the PHI retained? To what extent do HIPAA rules (and training and compliance monitoring) apply?

Role of HR in Benefits Advocacy 2

- Option 2: Prevent HR access to any PHI—usually, again, with the exception of enrollment and eligibility information—from the TPAs, the Call Center and the Benefits Department
  - Need to train on covered and non-covered functions as in Option 1
  - Fewer complexities to the risk management training than for Option 1
  - No problems associated with PHI received by local HR
  - The need to assure that adequate mechanisms exist for resolving claims issues with the TPAs, Outsourcer and/or Benefits Call Center
    - Can be problematic if the Outsourcer is one of those that refuses to be a business associate
  - Not the option for the old, very decentralized manufacturing company or the high-tech company needing to provide high-touch service to retain employees
  - We haven't seen all of the pushback—not only from HR but from employees watching anxiously for benefits "take-aways"—resulting from attempts to implement this option yet. Stay tuned….

Role of HR in Benefits Advocacy 3

- Option 3: Bring some functions of local HR within the plan administration firewall
  - Significant additional training and compliance burdens for the Privacy Officer
    - Education and compliance monitoring necessary on many of the detailed rules of HIPAA
    - Systems, physical and administrative safeguards necessary at the local level
      - » Driven not just by compliance requirements but by risks associated with PHI kept by local HR acting on behalf of the group health plans
- Common to all 3 options above:
  - Enrollment and eligibility information is treated as subject to—at least—lesser protection than claims-related information, and is available to local HR
    - Based in part on the argument that this information is generated by the employer or sponsor rather than the group health plans, as an employer or settlor function

HR Privacy Beyond HIPAA

- If not HIPAA privacy, should broader privacy rules apply to local HR, employee health services, and non-covered programs (e.g., disability, leaves of absence)?
  - The likelihood of confusion CAUSED in part by HIPAA Notices of Privacy Practices about the privacy of other health information such as disability, workers' comp, employee health services, drug-testing, work-related physicals, FMLA and ADA drives a focus on the privacy of employee HEALTH information more broadly than HIPAA.
    - The most common non-HIPAA HR privacy policies focus on health information
  - Yet since 9/11, HR privacy legislation in the states and privacy litigation have generally not been focused on health issues at all. Rather they have dwelt primarily on broader workplace privacy issues such as email screening, surveillance and background checks.
    - So will we see movement in this country toward privacy policies focused on the privacy of PERSONAL information as in the European Union?
      - » Or is that issue too "French" for us?"

Governmental Employers and HIPAA

- Suddenly, ERISA concepts like “plan,” “plan sponsor” and “plan documents” that have never applied to governmental and church plans before are imposed on both
  - Is the “plan” a separate entity, as are private ERISA plans?
  - If not, is the plan merely a covered component of a hybrid entity?
    - If so, need the plan documents be amended?
  - Is the government as a whole the sponsor, or is the agency that administers the plan?
    - If the government as a whole, need the plan documents be amended?
  - Is the agency that administers the plan a business associate of the plan?
    - If so, need the plan documents be amended?

Change at the Fringes: Typical "Borderline" Cases

- Employee Assistance Program (EAP)
  - Is it a welfare plan, and therefore a group health plan?
    - Does it provide short-term counselling, or just information and referral services?
  - If it is a group health plan, does its management referral process involve an invalid (coercive) authorization given by the EAP to the employee at intake?
  - Will the EAP:
    - Accept responsibility as an independent covered entity?
    - Insist on business associate status?
    - Deny that HIPAA applies at all?
  - Can the EAP respond to requests for access, amendment, accounting of disclosures?
- Executive Physical Programs
  - Is it a welfare plan, and therefore a group health plan?
    - Is it mandatory, like a drug screening, or a benefit?
  - Is information concerning fitness for duty disclosed to HR/management?

A Few of the Many Questions for After April 14th

- What will happen to the self-funded employers—if any—that don't even issue a Notice of Privacy Practices or take a stab at the other public-facing indicia of HIPAA compliance?
- How many employees, covered dependents or attorneys will assert HIPAA privacy rights?
- Who are the enforcers to watch?
- What is the political appetite for broader privacy regulation than HIPAA?
- Standard Transactions: Given that the 834 and 820 are not regarded as required for employers, will they begin to look generally attractive as platforms for consumer-directed healthcare or interchangeability of benefits more generally, once there are tested solutions?
- Security: How big a burden will it be for plan sponsors that receive PHI?
  - Due to the absence of cross-certificates, most plan sponsors that get PHI send it by unencrypted email.

For more information on the content of
this presentation, please contact:

Jon Neiditz
(678) 419-1556
jonathan.a.neiditz@us.pwcglobal.com