PRICEWATERHOUSECOOPERS

# Managing the Privacy of Employee Health Information

The privacy of employee information has joined the privacy of consumer data as a focus of privacy programs for companies both in the US and abroad. In the US, that issue is being driven for health information primarily by HIPAA's privacy rules.

A rapidly developing patchwork of employee privacy regulation around the U.S. and abroad presents a significant challenge to the management of multi-state and international workforces. Risk management around employee privacy has become a factor to consider in designing human resources and benefits strategies, developing policies, procedures and controls, and in choosing and implementing technology-based HR systems.



DLDL02-1153

## The U.S. and the HIPAA Privacy Rules

The most compelling basis for addressing employee privacy issues in this country are the privacy rules issued under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The intent of the Administrative Simplification provisions was to promote the affordability of health care services and insurance coverage through streamlining administrative operations, most notably through standardized electronic transactions and code sets; controls on the privacy and security of health information were included as a prerequisite to the free flow of health information in electronic commerce. Since HIPAA was enacted, however, the emergence of the internet heightened the political profile of the privacy issue. Complex privacy rules were issued December 2000 by the Clinton Administration and finalized by the Bush Administration in April 2001. For most employers, it is the privacy component of HIPAA that will demand the lion's share of their compliance efforts.

HIPAA privacy regulation may represent the most detailed set of requirements to which employee health benefits have ever been subjected, but it can be summarized generally as requiring that all employers offering health benefits implement the following measures before April 14, 2003:

- Securing (both physically and technically) records containing individually identifiable health information so that they are not readily available to those who do not need them.
- Separating benefit 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.
- Designing and adopting clear privacy procedures, and training affected employees on them.
- Designating an individual (the privacy officer) to be responsible for seeing that the privacy procedures are adopted and followed.
- Identifying and contracting with all business associates regarding adherence to privacy rules, and taking action if a violation is known.
- Establishing processes for employees to access and amend their protected health information, as well as to receive accountings of disclosures of that information.
- Providing complaint and remediation processes.

*- more -*

- cont. from pg 1 -

Although there are considerable regulatory penalties for noncompliance, it is unlikely that the regulators will proactively enforce the HIPAA rules against employers outside of the healthcare and health insurance industries (except in the context of whistleblower reports). Employers are generally more concerned about civil liability in state court actions–for example, for wrongful termination or breach of fiduciary duty–using national HIPAA standards as a considerably higher "floor" for the privacy of employee health information. Avoidance of negative media exposure and employee relations problems also factor into employers' decisions to address the privacy of health information.

## Covered Entities Under HIPAA

The employer is not an entity covered under HIPAA. Rather, the employer's "health plans" are covered, including:

- Medical Benefit Plans
- Prescription Drug Plans
- Most EAPs
- Long Term Care Plans
- Dental Plans
- Vision Plans
- Flexible Spending Accounts
- Personal Health Accounts

In addition, some of the clinical services provided directly by employers to their employees may constitute covered providers under HIPAA (if they engage in HIPAA's standard transactions and exceed *de minimus* exceptions). Indirectly impacted by HIPAA are all "business associates," that use the protected information of covered entities for or on behalf of those entities.

## Information Protected and Areas of Employer Exposure

HIPAA defines protected health information (PHI) very broadly, to include any information, whether in electronic, printed or spoken form, that identifies or could be used to identify an individual and relates to either the past, present, or future health or condition (physical or mental), the provision of health care; or the past, present, or future payment for the provision of healthcare. Particularly noteworthy for an employer is that such information is PHI if it is created or received either by a covered entity or by an employer.[1] To be sure, the detailed requirements of the HIPAA rules apply only to HIPAA's covered entities, but employers are probably right to be concerned that any individual health information created or received by an employer can be accurately characterized–in the state court actions and media pieces they anticipate–as information protected under federal law.

The breadth of the definition of PHI, as well as more stringent requirements of state law–that are preserved and made more visible by HIPAA–lead many employers to look beyond PHI in covered entities to programs that use health information on employees, particularly when that health information is combined with performance information. The scope of HIPAA reviews often include, for example:

- Health & Productivity Programs
- Health Promotion/Disease Prevention
- Workplace Health & Safety Surveillance
- Individual Risk Appraisals & Fitness for Duty Exams
- Absenteeism Studies & Absence Management ProgramsIntegrated Disability Programs

In addition, investigative procedures and coverage documents in "non-covered" areas such as disability and life insurance often need to be changed because of the stringent rules HIPAA imposes on the health care providers from which the information must be sought.

## Firewalls

HIPAA requires that self-insured employers create new "firewalls" around its covered benefit plans, through new policies, procedures and controls, amendment of plan documents and training of employees. Generally, the employer as plan sponsor may only receive information from the covered group health plan or its vendors if it assures that the information will only be used for plan administration purposes–rather than employment-related purposes or functions relating to other plans–and modifies its plan documents to that effect. 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.

[1] See the definitions of "individually identifiable health information" (IIHI) and "protected health information" (PHI) under 45 CFR §164.501. Dr. Bill Braithwaite, who oversaw the rules from their inception and is now a member of the PricewaterhouseCoopers HIPAA practice, confirms that the reference to "employer" in the definition of IIHI, that flows through to the definition of PHI, was regarded by Department of Health and Human Services as an unfortunate necessity given the "error" of the retention of the word "employer" in the applicable section of the HIPAA statute.

## New Individual Rights Create New Administrative Challenges

Self-insured employers should be aggressively questioning their third party administrators (for most employers, their highest-exposure "business associate") about the extent to which those administrators will fulfill the many administrative duties imposed on covered plans by HIPAA (many of which are associated with new individual rights), how they will do so, and whether they will offer the employers indemnification regarding their performance of those duties. Those duties include:

- Providing employees and dependents with access to a "designated record set" of their own PHI
- Allowing them to amend that designated record set (the plan may deny the request but must then allow the individual to place an explanation in the record)
- Ensuring that individuals may receive an accounting of non-exempt disclosures of PHI over the past six years (at a minimum)
- Ensuring that individuals may request restrictions on use or disclosure of their PHI (though such requests need not always be granted)
- Ensuring that communications are made by an alternative means or at alternative location when requested
- Providing detailed notices of privacy practices

## A Major Issue Associated with International Requirements

In Europe, as well as in Australia, New Zealand, Hong Kong and some Latin American countries, the privacy of employee health information is regulated under much more general privacy laws regulating all personal information in the employment context or otherwise.

Many U.S.-based multinationals are particularly concerned about the European Union issue commonly known as "transborder data flows." Within Europe, existing privacy legislation places restrictions on the transfer of personal information to countries outside the EU that do not meet the EU's privacy standards. Companies located in countries that fail to satisfy this requirement are subject to injunctive measures such as the blocking of all dataflows as well as criminal and civil sanctions. The U.S.'s less comprehensive approach to privacy protection is not deemed by the EU to meet its adequacy requirements. Thus U.S. corporations complying with the more detailed and stringent requirements of HIPAA for health information could face the ironic result that dataflows regarding health information could be prohibited by the EU. Any companies operating international HR systems that centrally warehouse HR data in an "unregulated" country such as the U.S. are held to the same restrictions. There have already been several publicized cases of companies that have breached the transborder data flow requirements in an HR context and suffered financial losses and reputational damage at the hands of EU enforcement bodies. Moreover, other countries continue to model their privacy laws on that of the EU, so the issue will probably not be limited to Europe.

## Conclusion

Facing the double threat of HIPAA privacy regulation and limitations on transborder data flows, and anticipating more activity on employee privacy by legislatures and the courts at home and abroad, U.S. corporations need to implement an employee privacy program. Yet such a program must balance risks associated with civil liability, regulatory enforcement, negative media exposure and employee relations problems against considerations such as ease of administration, cost containment, productivity, valuable information about employees and employee satisfaction/retention. Employers need practical solutions that satisfy the former goals without sacrificing the latter.

## *About the Authors:*

Jeffrey P. Fusile, is national partner in charge of HIPAA Consulting Services and an author of "HIPAA's Myths, Practical Realities and Opportunities" published by PricewaterhouseCoopers. From his Atlanta base, Fusile assists some of the nation's largest healthcare enterprises in addressing administrative simplification provisions of HIPAA. Before assuming leadership of HIPAA Consulting Services, Fusile served as PricewaterhouseCoopers' national director for Regulatory Consulting Services to the health insurance industry. He is a member of the advisory council for the Privacy Officer's Association, and has provided testimony before the National Council for Vital Statistics (NCVHS). Jeff can be reached at (678) 419-1558, or jeff.fusile@us.pwcglobal.com.

Jonathan Neiditz, J.D, is a nationally recognized legal expert on HIPAA privacy issues, and leads privacy initiatives with major U.S. employers, managed care organizations and government agencies. During his 17-year career as a general counsel and consultant, Neiditz also has contributed to health reform through work with the Jackson Hole Group, public health leaders and state governments. Neiditz has directed privacy and HIPAA assessments and implementations for such clients as Aetna, Ford, ValueOptions and the Commonwealth of Puerto Rico. Neiditz serves as a director of many innovative health and research organizations, and as adjunct faculty at Emory University's Rollins School of Public Health. Jon can be reached at (678) 419-1556, or jonathan.a.neiditz@us.pwcglobal.com

This article was originally published in the "Privacy Officer Advisor" the official publication of the International Association of Privacy Officers. For additional information on the International Association of Privacy Officers, please go to www.privacyassociation.org.