EPLiC™

Employment Practices Liability Consultant

"Your quarterly guide to exposures, coverage, and loss control"

Summer 2003

The Next Hurdle for EPLI? Privacy Issues under HIPAA

By Peter R. Taffae

On April 14, 2003, the United States Department of Health and Human Services began enforcing the privacy provisions applicable under the Health Insurance Portability and Accountability Act (HIPAA), an event that is almost certain to begin placing employers at risk of lawsuits.

Sponsoring health plans with $5 million or more in annual receipts must immediately comply with the privacy provisions of HIPAA; all others will have until April 14, 2004. The measurement of "annual receipts" varies according to the structure of the plan. For fully insured plans, "annual receipts" equal the premiums paid during the prior fiscal year. For self-insured plans, "annual receipts" are the health care claims paid during the prior fiscal year. For partially insured plans, "annual receipts" are a combination of these two measures.

History of HIPAA

In early 1996, Congress passed HIPAA. The legislation was designed to improve the availability of health insurance coverage. In addition, HIPAA allows for the electronic transmission of patient health administration and financial data. Part of the legislation established and implemented security standards designed to protect the privacy of an individual's health and medical information. One of the most important aspects of HIPAA relates to the privacy of personal health information (PHI). The Department of Health and Human Services issued the privacy regulations in December 2000, providing standards for the protection of PHI. HIPAA does not preempt any state laws or regulations that may provide stricter privacy protections.

Substantial Compliance Burdens

An employer will have compliance obligations under HIPAA if a plan is self-insured or partially insured because the employer will create or receive PHI directly through its in-house benefits administrators, indirectly through a third-party administrator, or both. All employers subject to HIPAA are required, in part, to do all of the following.

- Designate a privacy officer
- Prepare HIPAA privacy policies and procedures
- Provide HIPAA training to in-house benefits administrators
- Notify employees of their HIPAA privacy rights
- Implement privacy safeguards for employee health information
- Negotiate "business associates" contracts that require third-party service providers to provide HIPAA privacy protections
- Amend all health plans to implement HIPAA's privacy safeguards

For a list of the 15 key compliance considerations for group health plans and, for each, an example of a group health plan provision or practice that would not comply with the laws and a tip on how to bring the plan into compliance, see www.dol.gov/ebsa/publications/top15tips.html.

Insurance Implications

While many companies are still trying to sort out their responsibilities under HIPAA, and while the Department of Health and Human Services (HHS) continues to issue "letters of interpretation," it remains

uncertain as to what extent HHS will utilize its power to bring litigation to enforce HIPAA's privacy regulations. HHS has stated that it intends to issue warnings to those companies not in compliance and reserves its right to litigate. Currently, litigation for violations under HIPAA is limited to HHS; however, private plaintiffs might also be allowed to bring actions in the near future. When that occurs, the likelihood of employee class actions will greatly increase.

We have already seen an outcry concerning HIPAA's privacy section. As recently as mid-April, a coalition of patient advocacy groups filed litigation seeking rescission of the privacy rules under HIPAA. The suit, filed in a federal district court in Philadelphia, charges that the HHS has turned the HIPAA privacy provisions into a "disclosure rule," thus adding to an already confusing new law.

At this stage, insurance underwriters are trying to figure out the implications of HIPAA's privacy rules and HIPAA compliance standards and are determining how their policies might be affected. Following is a brief review of potential insurance coverage available under employment practices liability insurance (EPLI) policies.

Coverage for HIPAA Claims under Employment Practices Liability Insurance (EPLI) Policies

An analysis of EPLI policies currently available on the market suggests that claims by employees alleging privacy violations should be covered by such forms. This position is based on the philosophy that the spirit of a comprehensive EPLI policy is to protect the insured organization against litigation arising out of errors and omissions associated with the employment process, of which the administration of employee health care programs is an integral part.

To assess the extent of coverage provided by the EPLI policies available in the current marketplace, we reviewed the top 10 forms. In evaluating whether an allegation of "privacy violations" made by employees against the insured organization would be covered, one should look at a policy's definitions of "Wrongful Act" and "Claim," as well as the policy's reporting provisions.

Unfortunately, the majority of the forms reviewed do not include "invasion of privacy" within their definition of "Wrongful Act." Moreover, a number of these policies also require, within their definition of "Claim," that the allegation be made as part of a "formal administrative or regulatory proceeding," which is also restrictive. In addition, coverage for claims alleging a violation of privacy in conjunction with the administration of an employee benefit plan could be precluded by the standard ERISA exclusion found in most EPLI forms. Accordingly, a "carve out" of the exclusion, which would provide coverage for this exposure, needs to be made. Finally, none of the policies reviewed, except for one, include any coverage for the breach of privacy arising out of:

> Internet, e-mail, telecommunications or similar systems including failure to provide and enforce adequate policies and procedures.

However, due to the HIPAA provision allowing for the transfer of medical records via the Internet, along with the Act's privacy provisions, there can be substantial exposure to claims resulting from the unauthorized access of records by employees (including ex- and disgruntled employees), as well as by hackers/crackers.

Although this preliminary survey of policy forms and underwriters resulted in the recognition of exposures associated with HIPAA, there have been no final underwriting decisions on how to address this potentially massive litigation concern. A number of underwriters are currently undecided about whether they want to cover or exclude violations of HIPAA and/or allegations of privacy violations. Others have clearly expressed that they do not want to become involved with this new exposure.

Concluding Thoughts

Despite such reservations, we believe their concerns can be alleviated and the exposure effectively underwritten. The legislation is explicit regarding the expectations of HHS. In addition, HIPAA is quite clear about the actions that need to be taken to comply with its regulations. Accordingly, we suggest that by asking several specific questions on a supplemental application, underwriters would be able to make an informed decision concerning the extent of a prospective insured's susceptibility to claims associated with this new and important exposure. EPLiC

Peter R. Taffae is president of e-perils.com Insurance Services, an independently owned national wholesale broker that specializes in directors and officers (D&O), employment practices liability (EPL), cyber, legal malpractice, crime, fiduciary liability, and errors and omissions (E&O or executive perils) insurance. Mr. Taffae is also a member of the EPLiC editorial board. He can be reached at (310) 444–9333 or petert@e-perils.com. Web site: www.e-perils.com