

**August 2002 - Issue 1**

SDA is pleased to introduce *Issues in Brief*, a new information resource for our members. From time to time, we'll invite professional experts in our membership to share information of special interest.

## **Practical Tips for Developing a Medical Privacy Program**

**By Penny Wofford  
Edwards Ballard Law Firm**

Employers who sponsor health plans will soon be required to have in place a program to safeguard health information. The final privacy rule issued by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) in December 2000 requires health plans, healthcare clearinghouses, and healthcare providers to reasonably safeguard individually identifiable health information, including oral information, from use or disclosure that is in violation of the rule.

Basically, the rule prohibits an employer-sponsored health plan from using or disclosing an individual's health information for purposes other than treatment, payment or health care operations--absent a special written authorization from the individual. In addition, the rule imposes comprehensive requirements to ensure that health plans implement the appropriate physical, technical, and administrative safeguards to protect health information from unauthorized use or disclosure.



**Penny Wofford**

### **Administrative Requirements**

The privacy rule requires health plans to:

- Adopt clear written privacy policies and procedures;
- Designate a privacy officer to be responsible for ensuring the policies and procedures are followed;
- Provide a notice to plan participants about their privacy rights and how their health information may be used by the plan;
- Train employees with access to health information on the plan's privacy policies and procedures; and
- Develop a mechanism to allow participants to request copies of their health information maintained by the plan, request amendments to the records, and an accounting of disclosures made by the plan.

## **Business Associates**

The privacy rule requires business associates of health plans to agree through contract to safeguard protected health information. A business associate is any person or organization who provides services to the health plan, including legal, actuarial, accounting, consulting or administrative services. Employers are required to ensure specific information required by the rule is included in written contracts with any business associate that performs services for the health plan.

## **Deadlines For Compliance**

Most health plans must be in compliance with the privacy rule by April 14, 2003. However, employers who sponsor small health plans (defined as plans with annual receipts of \$5 million or less) have until April 14, 2004, to comply with the rule.

The Department of Health and Human Services has issued guidance and finalized revisions to the rule and has indicated that it will issue future technical guidance on an ongoing basis as questions arise. However, Congress set the compliance deadlines in the HIPAA legislation and there is no indication that they will be extended. ***The rule is comprehensive and much time will be required to implement a fully compliant privacy program.*** The bottom line is that the deadlines are fast approaching and employers must start now to achieve compliance by the deadlines.

## **Steps for Getting Started**

The guidance issued by the Department contemplates that privacy policies and procedures should be based on the volume of health information maintained by a particular health plan and the number of interactions with those outside of the entity. Hence, the policies and procedures of a smaller employer may be more limited than that of a large employer with a large health plan. Regardless of the size of your organization's health plan, the following steps will help get your plan well on its way to implementing a compliant program:

- Appoint a privacy officer and provide training for the officer on the nuances of the rule. Many trade associations and human resources or professional organizations are or will be offering comprehensive seminars or education programs on the specific requirements of the final rule.
- Analyze how health information flows within your organization. Based on your analysis, begin a draft of your organization's policies and procedures. Look first for simple safeguards to implement. Physical barriers such as locks for file cabinets or password protection for electronic data are fairly simple to address.
- Inventory contractual relationships with business associates and chart the deadlines for each contract's renewal so that you include the necessary privacy information in the contract. The proposed revisions issued by the Department include model business associate contract provisions.
- Develop or revise current forms and policies to comply with the specific requirements of the privacy rule.

- Design a training plan for employees who receive or use protected health information within your organization. Training for smaller health plans may simply include an oral overview of the organization's policies and procedure while training for a larger health plan may require a live presentation or an interactive software program.

For answers to specific questions regarding the privacy rule or developing your organization's privacy program, you may contact Penny Wofford at the Edwards Ballard Law Firm. Telephone: (864) 542-8612. In addition, the Department of Health and Human Services has published its guidance and proposed revisions to the privacy rule on its website at <http://www.hhs.gov/ocr/hipaa/>.

**This fall, the SDA will sponsor a HIPAA workshop on the final privacy rule for employers and health care providers. The workshop will focus on everyday situations faced by employers and health care providers that implicate the rule as well as on drafting forms and policies to meet the requirements of the rule. SDA members will soon receive details.**