



CIS (CAN INSURANCE SERVICES) IS A SUBSIDIARY OF THE CALIFORNIA ASSOCIATION OF NONPROFITS

Another Heap-a HIPAA

All Small Health Plans Must Comply by April 20, 2006

By Debbie Klug, Research & Compliance, CAN Insurance Services

Just when you got comfortable complying with HIPAA's Privacy rules, along comes the next phase...*security*.

To refresh your memory (also see our spring 2004 newsletter), HIPAA, the Health Insurance Portability and Accountability Act of 1996, is broad, Federal legislation with provisions to improve the privacy and security of individual health information.

Small health plans (those employers paying \$5 million or less per year in premiums or contributions toward group health care) were required to comply with the privacy provisions by 4/14/04. Depending upon how much access the health plan (in most cases—the employer) had to protected health information (PHI), this included naming a Privacy Officer, establishing Business Associate Agreements, creating privacy policies and procedures, creating a privacy notice, and training your staff, among other things. Penalties for noncompliance range from \$100–\$250,000 and up to 10 years in prison!

Now all small employers are required to comply with the HIPAA Security Rule by **April 20, 2006**. It's important to understand that these security provisions only apply to **electronic PHI** (ePHI) that is created, transmitted or maintained by an employer.

Do you deal with ePHI? Ask yourself the following questions:

Do you create any computer spreadsheets regarding your employees' healthcare? = ePHI

Do you receive an emailed itemized bill for your employees' health insurance? = ePHI

Do you use email to correspond with outside sources regarding your employees' healthcare (e.g. asking for assistance with a claim or billing, enrollments, terminations, etc.)? = ePHI

Do you use any kind of "online" enrollment program? = ePHI

Do you discuss Flexible Spending Account (FSA) reimbursements with your Third Party Administrator (TPA) via email? = ePHI

If you were able to answer "no" to all the questions above—congratulations! By doing things the old-fashioned way, with paper faxes, hard copy records and phone calls, you will have fewer hoops to jump through in order to comply.

HIPAA Requirements

The HIPAA Security Rule requires that all health plans meet four general requirements:

- 1** Ensure the confidentiality, integrity and availability of all ePHI that the plan creates, receives, maintains, or transmits
- 2** Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- 3** Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the HIPAA Privacy Rule
- 4** Ensure compliance with the HIPAA Security Rule by the health plan's workforce

HIPAA continued on page 2

However; due to the dynamic changes in technology, more and more health information is moving away from paper processes (such as hard copy applications) and is relying on computer based programs (such as on-line enrollment). While this may increase efficiency, the potential security risks are numerous.

In any case, all employers are going to have to complete some required tasks of the new Security Rule including: designating a Security Officer, completing a security risk assessment, and periodic assessment of its security measures. If you are insured through CIS and have limited access to ePHI (“hands off”), we have the following tools available to assist with HIPAA Security compliance:

- Our HIPAA Privacy newsletter article (*Spring 2004*)
- Risk Analysis Matrix
- Business Associate Agreement Security Addendum
- “Hands off” Security Policy
- Security Officer Roles and Responsibilities
- HIPAA Common Terms and Definitions

Please email us at info@caninsurance.com if you would like any of these materials. For additional information on HIPAA Security, visit www.cms.hhs.gov/HIPAAGenInfo/.

For those employers who have more extensive interaction with ePHI, we recommend you seek legal or expert advice on how to comply with the Security Rule. You may wish to visit www.ohi.ca.gov/state/calohi/ohiHome.jsp and click on Links.

This article is an outline of the basic responsibilities of employers under HIPAA Security. We recommend, because of the complexity and potential liability of HIPAA, legal advice or other expert assistance be obtained. ■

HIPAA Security Compliance Roadmap

What you have to do to comply with the newest HIPAA Rule:

- 1 Appoint a Security Officer (may be the same person as the Privacy Officer)
- 2 Review the standards matrix to see which implementation specifications are required vs. addressable
- 3 Perform a security risk assessment and develop a plan to address any gaps
- 4 Document all decisions (e.g. on addressable specifications, did you implement? Why not?)
- 5 Add security requirements to Business Associate Agreements
- 6 Develop security policies and procedures appropriate for your organization
- 7 Train all workforce (initial and ongoing)

