



## Don't be in a "HIPAA" trouble come April 14

### *New health privacy rules affect even small nonprofits*

By Debbie Klug, Research & Compliance, CAN Insurance Services

Have you ever wondered what happens to your private health information (PHI) after an examination, surgery, or survey has been completed? Consider these horror stories:

- *A copier repairman viewed PHI for numerous employees on an unattended monitor when using the phone in an office.*
- *Thousands of health claim forms blew out of a truck on its way to a recycling facility.*
- *Someone purchased a used computer containing prescription records.*
- *Pharmaceutical companies sold marketing lists containing the names of millions of elderly, incontinent women.*
- *A banker who sat on a county health board agency gained access to patients' records and identified several people with cancer, then called their mortgages.*

HIPAA, the Health Insurance Portability and Accountability Act of 1996, is broad, Federal legislation with provisions to improve the privacy of individual health information. The regulation was designed to impose new privacy and security requirements (e.g. who has access to your personal health information and who they can share it with).

While most of the new rules and regulations fall on the shoulders of insurance carriers, there are new responsibilities for all employers, including nonprofit organizations. If your organization pays less than \$5 million annually in premiums or contributions toward your employee's health-related benefit plans, you are considered a *small health plan* and must comply with certain privacy provisions of the act by April 14. (*Some exceptions may apply, please contact your legal counsel, health plan provider or CAN Insurance Services for details.*)

Don't panic! Following the steps below will have you well on your way to HIPAA compliance. The regulations vary significantly, depending on how much access you have to your employee's PHI (protected health information), and what you do with it. For HIPAA compliance, most employers will generally fall into one of two categories or groups, referred to as "*hands off*" or "*hands on*".

Hands Off groups are defined as providing benefits through a contract insurance provider or carrier and ONLY receiving *summary health* and/or enrollment information. If a group health plan does not receive or maintain any employee's PHI, many of the administrative burdens required by the HIPAA privacy rules will not apply to the plan or plan sponsor, rather they become the responsibility of the insurer.

In contrast, "hands on" groups have access to employee's PHI (above and beyond the summary health and enrollment information) and therefore must implement numerous compliance procedures. A prime example of a "Hands On" group is one which provides a self-insured health plan or a flexible benefit plan.

HIPAA continued on page 2

# HIPAA: Common terms and definitions

**Authorization:** Written permission from an employee to allow PHI to be obtained/used for a specific purpose and for a specific amount of time.

*Example: If an employee wants assistance with a medical claim, you will probably need a written authorization from the employee before the provider or carrier will release any information.*

**Business Associate:** Someone who performs a function on behalf of your organization, is not an employee, and has access to PHI.

*Example: A lawyer with whom you have contracted to do legal oversight requests an employee's file to resolve a claim dispute.*

**Confidential communications:** When an employee requests communication regarding their PHI be made in a specific manner.

*Example: An employee asks that you don't mail information regarding their health plan to their home address, but rather to a P.O. box.*

**Minimum necessary rule:** Making reasonable efforts to limit the PHI you use, disclose or request to the minimum necessary to accomplish the task.

*Example: If an insurance carrier calls you with questions regarding an employee's recent surgery, only information regarding that particular surgery should be discussed.*

**Plan sponsor:** The employer (in most cases) that sponsors a health-related benefit plan.

**Privacy notice:** A notice describing your privacy practices for PHI.

**Protected Health Information (PHI):** Health information that identifies the individual to whom it relates.

*Example: A report showing employee social security numbers and descriptions of medical claims.*

**Small Health Plan:** An employer who pays less than \$5,000,000.00 annually in premiums or contributions toward employee benefit plans.

**Summary health information:** A summary of claim history, expenses or types of claims for your group with no way of identifying individual employees.

*Example: A report showing the total spent by your company in medical claims for a specific quarter.*

# Determine your agency's HIPAA privacy status

## Is your organization "hands on" or "hands off"?

If even one "hands on" item applies to your organization, you must comply with the majority of HIPAA's administrative standard procedures and follow the "hands on" requirements.

This may lead you to re-evaluate your need to access PHI. For example: do you really need to see your employee's medical questionnaire when they apply for coverage? Or could you have them place it in a sealed envelope for you to forward to your insurance carrier for processing? Such a simple step might save you a lot of time and effort with your organization's compliance responsibilities.

In order to assist our members, CAN Insurance Services has prepared a packet of sample forms pertaining to both Hands Off and Hands On organizations.

Packets may be obtained by contacting us at [info@caninsurance.com](mailto:info@caninsurance.com) or (888) 427-5222.

Hands Off sample documents include:

- Privacy officer roles and responsibilities
- Authorization for release
- Business associate contract
- Privacy policy/procedures

Hands On sample documents include:

- Plan Sponsor certification to group health plans
- Privacy officer roles and responsibilities
- Privacy policy
- How to determine whether plan documents should be amended
- Notice of privacy practices
- Authorization for release
- Business associate contract
- Privacy plan amendment
- Privacy policy use and disclosure procedures

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

Does your organization...?	Hands Off	Hands On
Assist employees with claim disputes and give assistance in understanding benefits (but only obtain PHI upon written authorization from the employee)?	✓	
Obtain summary health information (no PHI) from insurer for obtaining bids for coverage or modifying or terminating existing plan?	✓	
Have employees place completed applications for insurance which include a medical questionnaire in a sealed envelope before forwarding to carrier (so employer does not see PHI)?	✓	
Obtain detailed information from the carrier relating to enrollment for plan (but not containing PHI)?	✓	
Receive faxes or emails from insurance companies or providers containing PHI?		✓
Have access to databases containing PHI? or share access to PHI with business associates?		✓
Maintain a spreadsheet and/or reports with PHI?		✓
Receive applications including unsealed medical questionnaire directly from employees?		✓
Offer an employee health plan or flexible spending account (Section 125 plan) for which employer makes claim determinations (sees PHI)?		✓