



*Our mission is to provide information and strategies to business owners and managers for improvement in the effectiveness of its business management so that key objectives can be realized.*

CFO Plus, LLC

Ted Hofmann - Principal/Senior Consultant

John Morre - Principal/Senior Consultant

Linda Panichelli - Principal/Senior Tax Consultant

1450 Grant Avenue, Suite 102

Novato, CA 94945-3142

Home Office: 415-898-7879

Toll Free 866-CFO-PLUS or 866-236-7587

Email: [thofmann@cfoplus.net](mailto:thofmann@cfoplus.net)

[jmorre@cfoplus.net](mailto:jmorre@cfoplus.net)

[lpanichelli@cfoplus.net](mailto:lpanichelli@cfoplus.net)

Web: [www.cfoplus.net](http://www.cfoplus.net)

## HIPAA ABCs for Employers

Some have called it the "health hippo." This nickname is indicative of just how large and far-reaching this act of federal legislation is. The Health Insurance Portability and Accountability Act of 1996, or HIPAA, signifies change for many employers as well as health care organizations. The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing the various and unrelated provisions of this legislation, therefore HIPAA means different things to different people. One of the most common misconceptions is that HIPAA only applies to health care providers and insurance companies. This is not the case. The law applies to any employer that sponsors an employee benefit plan covered by ERISA, or the Employee Retirement Income Security Act. This benefit plan must also have 50, or more, participants or be administered by a third-party for the employer to be required to comply with its provisions.

HIPAA compliance focuses on Protected Health Information, or PHI. PHI includes any health care data, electronic or otherwise, that can be linked to a specific individual. The basic privacy principle suggests that organizations that possess personal information related to an individual's health care, or payment for it, can only disclose the information as outlined in the following scenarios:

- To the individual;
- Pursuant to a signed consent form necessary to carry out treatment, payment or health care operations; if not, then pursuant to a signed and narrowly crafted authorization;
- To the state or federal government for the purpose of public health, abuse/neglect investigations, etc.

Disclosing summarized data, which can not be linked to any specific individual, is generally acceptable.

HIPAA privacy regulations took effect on April 14 of this year for large health plans. Small health plans, or those with annual receipts of less than \$5 million, have an additional year to comply. It is important to note that the penalties for non-compliance can be steep. Violation of a single standard can result in penalties of up to \$25,000. Fines of up to \$250,000, and imprisonment, may be imposed for certain knowing violations. If you have already complied, be sure to keep up the good work. Remember to distribute privacy notices to new hires, to conduct regular training, and to ensure that service agreements with third party administrators and business associates are HIPAA compliant.

So, what is next? For those of you who are still struggling to comply with this year's privacy rules, you may not be thrilled to hear about the new security rules. Security regulations go into effect on April 21, 2005, for large plans, and April 21, 2006, for small plans. These regulations have a more narrow focus and apply only to electronic PHI. Remember, the privacy rules apply to PHI in any form.

Electronic PHI includes any information stored in, received or sent by a computer (email), as well as phone voice response and faxback systems. However, information transmitted by telephones including person-to-person phone calls, paper-to-paper facsimiles, and voicemail messages is not covered.

The new rules do not require the use of any particular security measures but the regulations do set forth a number of required standards, along with implementation specifications for each standard. Administrative, physical and technical safeguards must also be implemented in order to protect electronic PHI.

## HIPAA ABCs for Employers (cont.)

- Administrative safeguards include items such as developing policies and procedures regarding workplace security and information access
- Physical safeguards include such items as policies and procedures regarding limiting access to facilities, as well as computer workstations
- Technical safeguards involve the implementation of access control mechanisms and methods to preserve data integrity

Even though the security rules compliance date for HIPAA is a long way off, taking action now may not be a bad idea. Adding information systems representatives to your HIPAA compliance team is a good start. Also, get a copy of the security matrix set forth in the regulations. It will serve as a checklist for evaluating your organization's compliance with each standard. By determining exactly what you already have in place, you can then easily identify the changes necessary for you to ensure HIPAA compliance in the future. If you aren't sure what to do next, give us a call. We'll walk you through the HIPAA maze.