



Dynamic Chiropractic – February 24, 2003, Vol. 21, Issue 05

The Deadline for Compliance With the HIPAA Privacy Rules Is Approaching

By Andrew, D., Esq. Bershad

The Department of Health and Human Services (HHS) has promulgated the regulation entitled, *Standards of Privacy of Individually Identifiable Health Information*, i.e., "The Privacy Rules," which becomes effective on April 14, 2003. The Privacy Rules create national standards to protect individuals' medical records and other personal information, and are designed to:

- give patients more control over their health information;
- set limits on the use and release of health records;
- establish appropriate safeguards that health care providers and others must implement to protect the privacy of health information; and
- hold violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.

This regulation was required because in enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of standards for the privacy of individually identifiable health information. As required by HIPAA, "covered entities" under the Privacy Rules include health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions that involve the electronic or paper transmission or maintenance of health care information. These entities are bound by the new privacy standards even if they contract with others to perform some of their essential functions. Under the HIPAA Privacy Rules, there is a distinction between an employer and its health plan. While the health plan is a "covered entity" directly regulated by the Privacy Rules, the employer is not a "covered entity," and therefore will only be indirectly subject to the Privacy

Rules.

As required by HIPAA, most "covered entities" have until April 14, 2003, to comply with these standards.

For "covered entities" with gross receipts under \$5 million, the compliance date is April 14, 2004.

Therefore, "covered entities" that have not yet taken steps to comply with the Privacy Rules must promptly address their requirements. For most health care providers or health plans, the Privacy Rules require certain activities, such as:

- providing information to patients about their rights of privacy, and how such information can be used;
- adopting clear privacy procedures for a practice, plan or hospital;
- training employees to understand the privacy procedures; and
- securing patient records containing individually identifiable health information, so that they are not readily available to those who do not need them.

To ease the burden of complying with the new standards, the Privacy Rules give some flexibility to providers and plans to create their own privacy procedures, based upon their size and needs. As examples:

- In a small physician practice, the privacy officer may be the office manager, who will have other non-privacy-related duties; on the other hand, the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
- The training requirement may be met by a small physician practice providing each new employee with a copy of its privacy policies and documenting that new employees have reviewed the policies; a large health plan may provide training through live instruction, video presentations or interactive software programs.
- The policies and procedures of small providers may be more limited under the Privacy Rules than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside the health care system.
- The penalties for noncompliance with the Privacy Rules, however, are severe. The general penalty for violations is \$100 per violation, up to a maximum of \$25,000 per year per identical violation. Penalties for wrongful disclosure or use of "protected health information" can range from fines of \$50,000 to \$250,000, imprisonment from one to 10 years, or both.

Since most health care providers and health plans are "covered entities" that must comply with the new privacy standards by April 14, 2003, it is necessary to understand the requirements of the Privacy Rules and develop implementation strategies. HIPAA compliance must be met by the drafting of various documents, such as policies and procedures, authorization forms and plan amendments. In addition, compliance will require training of the appropriate employees and the development of enforcement policies.

Because employers differ with respect to the extent to which they need access to "protected health information," or with respect to the manner in which they administer their health plans, employers should take advantage of the flexibility allowed under the Privacy Rules to create their own privacy procedures. Therefore, employers and their health plans, as separate entities, should consider the following when developing compliance strategies:

- the extent to which it is necessary to have access to "protected health information" for purposes outside the scope of administration of the health plan;
- the extent to which employees have access to "protected health information" through internal administration of the health plan;
- the extent to which employees have access to "protected health information" when they have no legitimate need for such access; and
- where "protected health information" is stored (physically and electronically), and who has access to such information.

Andrew D. Bershad, Esq.

Philadelphia, Pennsylvania

Andrew D. Bershad, Esq., is Of Counsel to the Law Firm of Neal A. Jacobs & Associates, P.C., 1819 J.F.K. Blvd., Suite 300, Philadelphia, PA 19103. Please e-mail all comments or questions to the author at abershad@najlaw.com.



Page printed from:

http://www.chiroweb.com/mpacms/dc/article.php?id=9041&no_paginate=true&p_friendly=true&no_b=true