SEYFARTH SHAW
MANAGEMENT ALERT

February 2003

# HIPAA Electronic Security Regs Are Final

The final standards for the security of electronic protected health information (PHI) which must be followed by health plans, health providers and health care clearinghouses (Covered Entities) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) were released February 20, 2003 by the Department of Health and Human Services (HHS). Compliance with the security regulations is not required until April 21, 2005 for Covered Entities, other than small health plans that have an additional year to comply. However, under the HIPAA privacy regulations, Covered Entities are required to take steps to protect access to all forms of PHI by April 14, 2003, or a year later for small health plans Compliance with the privacy regulations with respect to electronic PHI is expected to meet many of the requirements of the security regulations.

HHS has also published modifications to some of the electronic transaction standards adopted under the electronic transactions regulations. Covered Entities that submitted EDI compliance plans by October 16, 2002 have until October 16, 2003 to comply, if transaction testing begins by April 16, 2003.

## *Electronic Security Standards*

Unlike the HIPAA privacy regulations, which affect PHI in any form, the electronic security regulations apply only to PHI in electronic form. While the electronic security regulations are intended to coordinate with the privacy regulations, the earlier effective dates for the privacy regulations (April 14, 2003, or April 14, 2004 for small health plans) mean that HIPAA privacy policies and procedures must take into account privacy measures for electronic PHI before the electronic security regulations' compliance date.

The security regulations offer a good blueprint. If many of the security regulations in the HIPAA privacy policy that Covered Entities must have, are reflected now, time and expense should be saved when final compliance with the electronic security regulations occurs.

As originally proposed, the electronic security regulations had 69 requirements. HHS considered the comments submitted and has presented 13 mandatory requirements considered so basic that no Covered Entity could effectively protect electronic PHI without implementing them. In addition to the 13 required standards, HHS adopted "addressable" implementation specifications which may be adopted as needed or appropriate for the Covered Entity in order to satisfy the required administrative, physical, technical, and organizational safeguards. This approach was intended to provide Covered Entities with added flexibility to comply based on the Covered Entity's particular environment, capabilities, and risk assessment. These factors may be different to the extent that electronic PHI is "outsourced" by a health plan, although the health plan would need to ensure compliance through its business associate agreement with the outsourcing firm.

A Covered Entity must decide whether a given addressable implementation specification will apply within its own security framework. If the Covered Entity determines that the implementation specification is reasonable and appropriate, the Covered Entity must adopt it. If the addressable implementation standard is determined to be inappropriate or unreasonable for the Covered Entity, then this must be documented by the Covered Entity and an alternate measure that accomplishes the same end must be implemented (if necessary to comply with the standard).

SEYFARTH ATTORNEYS SHAW

Other notable changes from the proposed electronic security regulations include:

- The "chain of trust" concept in the proposed regulations for contracts between partners trading electronic data is now rolled into the "business associate" contracts for the privacy regulations. The Covered Entity must obtain satisfactory assurance from its business associates that there will be appropriate safeguards for electronic PHI in accordance with the electronic security regulations. Health plans reviewing and entering into business associate contracts now in connection with the privacy regulations would do well to add language with respect to electronic security, even if not fully effective until 2005.

- Telephone voice response and fax-back systems are now considered to be electronic media subject to the electronic security regulations. As such, information transmitted via telephone is not considered electronic media, but information returned to a Covered Entity on a telephone voice response system is and will be subject to the electronic security regulations.

- There is no guidance on electronic signature standards; they will be published in separate regulations.

The fundamental requirements of the electronic security regulations are the requirements for a risk analysis, risk management and a sanctions policy. The risk analysis must identify the risks to and vulnerabilities of the PHI and will be the basis for determining the extent of adoption of the "addressable" specifications. Internal audit is now called "information system activity review" and is an integral part of the security implementation process. These steps will need to be taken before the 2005 compliance date for the electronic security regulations.

## *EDI Standards*

The standards for transaction and code sets to be used in the transmission of PHI have been revised and updated since the May 2002 proposed rules were issued. References to numerous websites for specific, technical information are also included in the regulations. Compliance testing should begin by April 16, 2003.

*If you have any questions about the application of these new regulations to your health plan, please contact the Seyfarth Shaw employee benefits group attorney with whom you work or any employee benefits group attorney listed on the website at www.seyfarth.com.*



ATLANTA
One Peachtree Pointe
1545 Peachtree Street , N.E., Suite 700
Atlanta, Georgia 30309-2401
404-885-1500
404-892-7056 fax

BOSTON
Two Seaport Lane, Suite 300
Boston, Massachusetts 02210-2028
617-946-4800
617-946-4801 fax

CHICAGO
55 East Monroe Street, Suite 4200
Chicago, Illinois 60603-5803
312-346-8000
312-269-8869 fax

HOUSTON
700 Louisiana Street, Suite 3850
Houston, Texas 77002-2731
713-225-2300
713-225-2340 fax

LOS ANGELES
One Century Plaza
2029 Century Park East, Suite 3300
Los Angeles, California 90067-3063
310-277-7200
310-201-5219 fax

NEW YORK
1270 Avenue of the Americas, Suite 2500
New York, New York 10020-1801
212-218-5500
212-218-5526 fax

SACRAMENTO
400 Capitol Mall, Suite 2350
Sacramento, California 95814-4428
916-448-0159
916-558-4839 fax

SAN FRANCISCO
101 California Street, Suite 2900
San Francisco, California 94111-5858
415-397-2823
415-397-8549 fax

WASHINGTON, D.C.
815 Connecticut Avenue, N.W, Suite 500
Washington, D.C. 20006-4004
202-463-2400
202-828-5393 fax

BRUSSELS
Avenue Louise 500, Box 8
1050 Brussels, Belgium
(32)(2)647.60.25
(32)(2)640.70.71 fax