

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Office of the Secretary

#### 45 CFR Parts 160, 162, and 164

[CMS-0049-F]

RIN 0938-AI57

### Health Insurance Reform: Security Standards

**AGENCY:** Centers for Medicare & Medicaid Services (CMS), HHS.

**ACTION:** Final rule.

**SUMMARY:** This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. This final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

**DATES:** *Effective Date:* These regulations are effective on April 21, 2003.

*Compliance Date:* Covered entities, with the exception of small health plans, must comply with the requirements of this final rule by April 21, 2005. Small health plans must comply with the requirements of this final rule by April 21, 2006.

**FOR FURTHER INFORMATION CONTACT:** William Schooler, (410) 786-0089.

#### SUPPLEMENTARY INFORMATION:

#### Availability of Copies and Electronic Access

To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512-1800 or by faxing to (202) 512-2250. The cost for each copy is \$10. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at

many other public and academic libraries throughout the country that receive the **Federal Register**.

This **Federal Register** document is also available from the **Federal Register** online database through GPO access, a service of the U.S. Government Printing Office. The Web site address is <http://www.access.gpo.gov/nara/index.html>.

#### I. Background

The Department of Health and Human Services (HHS) Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Currently, no standard measures exist in the health care industry that address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities.

This final rule adopts standards as required under title II, subtitle F, sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191. These standards require measures to be taken to secure this information while in the custody of entities covered by HIPAA (covered entities) as well as in transit between covered entities and from covered entities to others.

The Congress included provisions to address the need for safeguarding electronic health information and other administrative simplification issues in HIPAA. In subtitle F of title II of that law, the Congress added to title XI of the Social Security Act a new part C, entitled "Administrative Simplification" (hereafter, we refer to the Social Security Act as "the Act"; we refer to the other laws cited in this document by their names). The purpose of subtitle F is to improve the Medicare program under title XVIII of the Act, the Medicaid program under title XIX of the Act, and the efficiency and effectiveness

of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information.

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose requirements on HHS, health plans, health care clearinghouses, and certain health care providers. These statutory sections are discussed in the Transactions Rule, at 65 FR 50312, on pages 50312 through 50313, and in the final rules adopting Standards for Privacy of Individually Identifiable Health Information, published on December 28, 2000 at 65 FR 82462 (Privacy Rules), on pages 82470 through 82471, and on August 14, 2002 at 67 FR 53182. The reader is referred to those discussions.

Section 1173(d) of the Act requires the Secretary of HHS to adopt security standards that take into account the technical capabilities of record systems used to maintain health information, the costs of security measures, the need to train persons who have access to health information, the value of audit trails in computerized record systems, and the needs and capabilities of small health care providers and rural health care providers. Section 1173(d) of the Act also requires that the standards ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures that isolate the activities of the clearinghouse with respect to processing information so as to prevent unauthorized access to health information by the larger organization. Section 1173(d) of the Act provides that covered entities that maintain or transmit health information are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the officers and employees of the covered entities.

#### II. General Overview of the Provisions of the Proposed Rule

On August 12, 1998, we published a proposed rule (63 FR 43242) to establish a minimum standard for security of electronic health information. We proposed that the standard would require the safeguarding of all electronic health information by covered entities. The proposed rule also proposed a