(i) *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§ 164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.*

(1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

§164.500 [Amended]

6. § In 164.500(b)(1)(iv), remove the words ''including the designation of health care components of a covered entity''.

§ 165.501 [Amended]

7. In §164.501, the definitions of the following terms are removed: *Covered functions, Disclosure, Individual, Organized health care arrangement, Plan sponsor Protected health information, Required by law,* and *Use.*

§ 164.504 [Amended]

8. In §164.504, the following changes are made:

a. The definitions of the following terms are removed: *Common control, Common ownership, Health care component,* and *Hybrid entity.*

b. Paragraphs (b) through (d) are removed and reserved.

Authority: Sections 1173 and 1175 of the Social Security Act (42 U.S.C. 1329d–2 and 1320–4).

Dated: January 13, 2003.

Tommy G. Thompson,

Secretary.

[FR Doc. 03–3877 Filed 2–13–03; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 162

[CMS–0003–F and CMS–0005–F]

RINs 0938–AK64 and 0938–AK76

Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets

AGENCY: Office of the Secretary, HHS.

ACTION: Final rule.

SUMMARY: In this final rule, we respond to public comments received and finalize provisions applicable to electronic data transaction standards from two related proposed rules published in the May 31, 2002, **Federal Register.** We are also adopting proposed modifications to implementation specifications for health care entities and others. In addition, we are adopting modifications to implementation specifications for several electronic transaction standards that were omitted from the May 31, 2002, proposed rules.

EFFECTIVE DATES: These regulations are effective on March 24, 2003. The incorporation by reference of certain publications listed in this final rule is approved by the Director of the Federal Register as of March 24, 2003.

FOR FURTHER INFORMATION CONTACT: Gladys Wheeler, (410) 786–0273.

SUPPLEMENTARY INFORMATION:

Availability of Copies: 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 (toll-free at 1–888–293–6498) 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

A. Electronic Data Interchange

Electronic data interchange (EDI) refers to the electronic transfer of information in a standard format between trading partners. When compared with paper submissions, EDI can substantially lessen the time and costs associated with receiving, processing, and storing documents. The use of EDI can also eliminate inefficiencies and streamline processing tasks, which can in turn result in less administrative burden, lower operating costs, and improved overall data quality.

The health care industry recognizes the benefits of EDI, and many entities in the industry have developed proprietary EDI formats. However, with the increasing use of health care EDI standards, the lack of common, industry-wide standards has emerged as a major obstacle to realizing potential efficiency and savings.

B. Statutory and Regulatory Background

1. Statutory Background

The Congress included provisions to address the need for developing a consistent framework for electronic transactions and other administrative simplification issues in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, which became law on August 21, 1996. Through subtitle F of title II of that statute, the Congress added to title XI of the Social Security Act (the Act) a new part C, titled ''Administrative Simplification.'' The purpose of this part is to improve the Medicare and Medicaid programs in particular and the efficiency and effectiveness of the health care system in general, by encouraging the development 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. Section 1172 of the Act and the implementing regulations make any standard adopted under part C applicable to: (1) Health plans; (2) health care clearinghouses; and (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by 45 CFR part 162.

In general, section 1172 of the Act requires any standard adopted by the Secretary of Health and Human Services (the Secretary) under this part to be a standard that has been developed, adopted, or modified by a standard setting organization (SSO). The Secretary may adopt a different standard if the standard will substantially reduce administrative costs to providers and health plans compared to the alternatives, and the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, U.S.C.

Section 1172 of the Act also sets forth consultation requirements that must be met before the Secretary may adopt standards. In the case of a standard that is developed, adopted, or modified by an SSO, the SSO must consult with the following Data Content Committees (DCCs) in the course of the development, adoption, or modification of the standard: The National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). In the case of any other standard, the Secretary is required to consult with each of the above-named groups before adopting the standard and must also comply with the provisions of section 1172(f) of the Act regarding consultation with the National Committee on Vital and Health Statistics (NCVHS).

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable the electronic exchange of health information. Section