CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-04 Medicare Claims Processing	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 2517	**Date: August 10, 2012**
	Change Request 8004

SUBJECT: Medicare Claims Processing Pub. 100-04 Chapter 24 Update for Security Requirements

I. SUMMARY OF CHANGES: The purpose of this change request (CR) is to update the security provisions relative to the Medicare Claims Processing Pub.100-04 Chapter 24.

EFFECTIVE DATE: September 10, 2012
IMPLEMENTATION DATE: September 10, 2012

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	24/40.2.2 Security Requirements

III. FUNDING:
For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs) and/or Carriers:
No additional funding will be provided by CMS; Contractors activities are to be carried out with their operating budgets

For Medicare Administrative Contractors (MACs):
The Medicare Administrative contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC statement of Work. The contractor is not obliged to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements

Manual Instructions

**Unless otherwise specified, the effective date is the date of service.*

Attachment - Business Requirements

Pub. 100-04	Transmittal: 2517	Date: August 10, 2012	Change Request: 8004

SUBJECT: Medicare Claims Processing Pub. 100-04 Chapter 24 Update for Security Requirements

EFFECTIVE DATE: September 10, 2012

IMPLEMENTATION DATE: September 10, 2012

I. GENERAL INFORMATION

A. Background: The Centers for Medicare and Medicaid Services (CMS) is in the process of implementing the next version of the Health Insurance Portability and Accountability Act (HIPAA) transactions. The Secretary of the Department of Health and Human Services (DHHS) has adopted Accredited Standards Committee (ASC) X12 Version 5010 and the National Council for Prescription Drug Programs (NCPDP) Version D.0 as the next HIPAA transaction standards for covered entities to exchange HIPAA transactions. The final rule was published on January 16, 2009. Some of the important dates in the implementation process are:

Effective Date of the regulation: March 17, 2009

Level I compliance by: December 31, 2010

Level II Compliance by: December 31, 2011

All covered entities have to be fully compliant on: January 1, 2012

Level I compliance means "that a covered entity can demonstrate that it could create and receive compliant transactions, resulting from the compliance of all design/build activities and internal testing."

Level II compliance means "that a covered entity has completed end-to-end testing with each of its trading partners, and is able to operate in production mode with the new versions of the standards."

DHHS has promulgated in the Final Rules provisions which permit dual use of existing standards (ASC X12 4010A1 and NCPDP 5.1) and the new standards (5010 and D.0) from the March 17, 2009, effective date until the January 1, 2012 compliance date to facilitate testing subject to trading partner agreement.

The purpose of this CR is to publish an update to IOM Pub.100-04 Chapter 24 to reflect changes to Medicare Fee-For-Service's Electronic Data Interchange (EDI) practices, and corresponding EDI requirements for Medicare contractors that are being implemented as part of the 5010 implementation project.

As this is a no systems change CR, this is expected to be an In Scope change request.

B. Policy: CMS will implement the new HIPAA standard as adopted by the Secretary**.**Final Rules were published in the Federal Register on January 16, 2009, by the Department of Health and Human Services: 45 CFR Part 162.

II. BUSINESS REQUIREMENTS TABLE

Use "Shall" to denote a mandatory requirement.

Number	Requirement	Responsibility										
		A/B MAC		DME MAC	FI	CARRIER	RHHI	Shared-System Maintainers				Other
		Part A	Part B					FISS	MCS	VMS	CWF	
8004.1	Contractors shall implement all requirements contained within the IOM Pub. 100-04 Chapter 24 General EDI and EDI Support Requirements, Electronic Claims and Mandatory Electronic Filing of Medicare Claims	X	X	X	X	X	X					CEDI

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility						
		A/B MAC		DME MAC	FI	CARRIER	RHHI	Other
		Part A	Part B					
	None							

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A
Use "Should" to denote a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Angie Bartlett, 410-786-2865 or angie.bartlett@cms.hhs.gov , Jason Jackson, 410-786-6156 or Jason.jackson@cms.hhs.gov , Sumita Sen, 410-786-5755 or sumita.sen@cms.hhs.gov

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR) or Contractor Manager, as applicable.

VI. FUNDING

Section A: For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs), and/or Carriers:
No additional funding will be provided by CMS; Contractors activities are to be carried out with their operating budgets

Section B: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS do not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

Medicare Claims Processing Manual

Chapter 24 – General EDI and EDI Support Requirements, Electronic Claims, and Mandatory Electronic Filing of Medicare Claims

Table of Contents

(Rev.2517, 08-10-12)

40.2.2 - Security Requirements

(Rev. 2517, Issued: 08-10-12, Effective: 09-10-12, Implementation: 09-10-12)

FIs, Carriers, RHHIs, A/B MACs, DME MACs, CEDI, and other entities contracting directly with CMS are considered service providers to CMS. As such, these entities are part of CMS' system security boundary and must be in compliance with the Federal Information Security Management Act (FISMA) and are subject to CMS security policies. Covered entities, trading partners and business associates not contracting as service providers to CMS are outside of the CMS system security boundary and are not considered as FISMA entities These entities must comply with the mandates of the HIPAA Privacy and Security Rules as well as the mandates defined in ARRA/ Health Information Technology for Economic and Clinical Health (HITECH).

A trading partner submitting an EDI Enrollment Agreement attests that it has executed Business Associate Agreements (contracts), as mandated by HIPAA and ARRA/HITECH, with each of its business associates. Moreover, the trading partner attests that it has full responsibility, as mandated by HIPAA and ARRA/HITECH, for notification of breaches of protected health information caused by the trading partner or its business associates.