Health Care Connecitivity Guide

Standard Companion Guide

December 6, 2022

Version 4.0

Disclosure Statement

The Kansas Department of Health and Environment (KDHE) is committed to maintaining the integrity and security of health care data in accordance with all applicable laws and regulations. This document is intended to serve as a connectivity companion guide for all ASC X12 transaction types and their related addenda and errata.

Disclosure of Medicaid Beneficiary eligibility data is restricted under the provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Provider Medicaid Beneficiary eligibility transaction is to be used for conducting Medicaid business only.

This document can be reproduced and/or distribute but it’s ownership by Kansas Medicaid must be acknowledge and the contents must not be modified.

Companion Guides may contain two types of data, instructions for electronic communications with the publishing entity (Communications/Connectivity Instructions), and supplemental information for creating transactions for the publishing entity while ensuring compliance with the associated ASC X12 Implementation Guide. Either the Communications/Connectivity component or the Transaction Instructions component must be included in every companion guide. The components may be published as separate documents or as a single document.

The Communications/Connectivity component is included in the companion guide when the publishing entity wants to convey the information needed to commence and maintain communications exchange.

Preface

This Companion Guide to the v5010 ASC X12N Implementation Guides and associated errata adopted under HIPAA clarifies and specifies the data content when exchanging electronically with Kansas Medicaid. Transmissions based on this companion guide, used in tandem with the v5010 ASC X12N Implementation Guides, are compliant with both ASC X12 syntax and those guides. This Companion Guide is intended to convey information that is within the framework of the ASC X12N Implementation Guides adopted for use under HIPAA. The Companion Guide is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the Implementation Guides.

Table of Contents

1. Introduction

Section 1104 of the Patient Protection and Affordable Care Act (ACA) establishes new requirements for administrative transactions that will improve the utility of the existing HIPAA transactions and reduce administrative costs.

Section 1104 of the ACA requires the Secretary of the Department of Health and Human Services (HHS) to adopt and regularly update standards, implementation specifications, and operating rules for the electronic exchange and use of health information for the purposes of financial and administrative transactions.

In compliance with this requirement, HHS designated CAQH CORE to be the authoring entity for the required rules. The CAQH CORE Operating Rules defined a Connectivity/Security Rule, which is a safe harbor that required the use of the HTTP/S transport protocol over the public internet. Since the CORE Phase 1 Connectivity Rule is a safe harbor, CORE-certified entities are required to support the adopted CORE Phase 1 Connectivity method at a minimum.

1.1 References

CAQH CORE Operating rules:

www.caqh.org/ORMandate_index.php

Phase II Core 270: Connectivity Rule version 2.2.0:

www.caqh.org/pdf/CLEAN5010/270-v5010.pdf

1.2 Scope

The instructions in this companion guide are not intended to be stand-alone requirements documents. This companion guide conforms to all the requirements of any associated ASC X12 Implementation guide and is in conformance with ASC X12's Fair Use and Copyright statements.

The information contained in this Companion Guide applies to the Kansas Medical Assistance Program (KMAP). KMAP will accept and process an HIPAA-compliant transaction; however, a compliant transaction that does not contain KMAP specific information, though processed, may be denied. For example, a compliant 270 Health Care Eligibility and Benefit Inquiry (270) created with an invalid KMAP member identification number will be processed by KMAP but will be denied. For questions regarding appropriate billing procedures, as well as for policy and billing information, providers should refer to the KMAP Customer Service department at 1-800-933-6593, option 6.

1.3 Compliance Version

KMAP is compliant with Phase II CORE 270: Connectivity Rule version 2.2.0 March 2011

2. Getting Started

This section contains payer-specific business rules and limitations for the Safe Harbor Connectivity. Users of the Safe Harbor Connectivity must obtain a Trading Partner ID and complete all necessary production testing.

2.1 Trading Partner Registration

Any entity wishing to become a KMAP Trading Partner for EDI transactions must first complete the EDI application found on the KMAP website at https://www.kmap-state-ks.us/Documents/EDI/KSEDIAP.pdf. Once the application is processed testing instructions will be sent to the potential submitter. After testing is successfully completed the Trading Partner will be given the necessary permissions to submit batches to our Production environment for processing.

3. Connection Details

3.1 KMAP Supported Transactions

KMAP supports batch and real time HIPAA X12 transactions of the Safe Harbor Connectivity.

The following transaction types are available as batch transactions:

1. Health Care Eligibility and Benefit Inquiry and Response (270/271).
2. Health Care Claim Status Request and Response (276/277).

The following transaction types are available as real time transactions:

1 Health Care Eligibility and Benefit Inquiry and Response (270/271).
2 Health Care Claim Status Request and Response (276/277).

3.2 Control Segments and Metadata Elements Definitions

The KMAP ASC X12 interchange rules and limitations will be unchanged from the web portal submission methods for all transactions supported over the Safe Harbor Connectivity. Refer to the specific transaction’s companion guide for details about functional group formatting.

CAQH CORE Operating Rule 270 specifies the data elements which should be present in the CORE envelope. The following are payer-specific requirements for the envelope metadata elements.

Element	Value
Sender ID	Trading Partner ID as supplied by the KMAP.
Receiver ID	‘00005’ – KMAP Trading Partner ID.
User Name	User name from KMAP website.
Password	Password from KMAP website.
Payload ID	Unique identifier for a submission. Must be unique for any batch or real-time transaction.
Payload Type	A standard payload type defined in section 4 of this guide.

3.3 Rules of Behavior

Partners transacting with us will agree to the following Rules of Behavior:

• All EDI transactions will follow the HIPAA format as established by CAQH governance.

• No partner will attempt to access patient eligibility, benefits or claims information unless they have a legitimate business reason for that information.

3.3.1 Passwords and Other Access Control Measures

• I will choose passwords that are at least eight characters long and have a combination of letters (upper- and lower-case), numbers, and special characters.

• I will protect passwords and access numbers from disclosure. I will not record passwords or access control numbers on paper or in electronic form and store them on or with workstations, or laptop computers. To prevent others from obtaining my password via “shoulder surfing,” I will shield my keyboard from view as I enter my password.

• I will promptly change a password whenever the compromise of that password is known or suspected.

• I will not attempt to bypass access control measures.

3.3.2 Data Protection

• I will protect sensitive information from disclosure to unauthorized persons or groups.

• All information received will be treated as PHI and fall under all requirements associated with privacy.

3.4 Maximum File Limitations

Real time EDI transactions are limited to a single concurrent transaction per user and no more than 60 transactions per minute for a trading partner.

3.5 Authentication/Authorization Policies

Currently the majority of trading partners who transact with KMAP for EDI messages do so through a secure web portal at https://www.kmap-state-ks.us. All trading partners are assigned a User Name and Password upon creation. For assistance with questions regarding a User Name or Password please contact KMAP Customer Service at 1-800-933-6593, option 8.

3.6 System Availability

The claims adjudication system and supporting transactions are monitored 24 hours a day, 7 days a week for the entire calendar year including holidays. We strive for 99.5% uptime with the exception of the following scheduled maintenance windows.

3.6.1 Scheduled Downtime:

Weekly - We maintain a short after hour downtime weekly for minor enhancements. These are scheduled for Fridays between 1 AM and 5 AM.

3.6.2 Unscheduled Downtime

Any unscheduled/emergency downtimes that affect our ability to reply to an EDI transaction will be communicated to necessary parties as soon as possible.

4. SOAP Interface

This section includes all the information necessary to develop a SOAP web service client/consumer for the EDIaaS HDE web service.

4.4 ACA Specification

Refer to the ACA document http://www.caqh.org/sites/default/files/core/phase-ii/policy-rules/270-v5010.pdf.for a specification of all of the EDIaaS HDE web service operations excluding changePassword. The ACA WSDL is available at *www.caqh.org/SOAP/WSDL/CORERule2.2.0.wsdl*.

4.5 EDIaaS HDE WSDL

The EDIaaS HDE WSDL can be obtained from a web browser with the URL:

https://hde.uat.oxisaas.com/OXiHDEServices/v1.0?wsdl

The EDIaaS HDE web service implements the above mentioned ACA CORE 270 Rule WSDL with the following modifications:

- Moved the external reference to the ACA types XSD http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd to be inline (defined within the WSDL).
- Added operation changePassword with an updated namespace.
- Updated the service endpoint URL and wsdl address location.
- Removed optional GenericBatch operations not implemented by the EDIaaS HDE web service

The WSDL includes the following operations:

Table 1 – EDIAAS HDE Web Service Operations

Name	Description
RealTimeTransaction	Submit real-time 270 and 276 requests
BatchSubmitTransaction	Submit batch 270 and 276 requests
BatchResultsRetrievalTransaction	Get batch 271/277 response for a previous BatchSubmitTransaction request
BatchResultsAckSubmtTransaction	Submit a TA1/999 for a previous BatchResultsRetrievalTransaction request.
BatchSubmitAckRetrievalTransaction	Get batch compliance check output 999 or TA1 for a previous BatchSubmitTransaction request.
changePassword	Change the HDE service security authentication password (MIME and SOAP service).

Refer to the ACA CORE 270 specification for documentation on all the above operations except for the EDIaaS added changePassword.

4.6 EDIaaS HDE Endpoints

Table 2 – EDIAAS HDE Web Service Endpoints

Env	Endpoint
SIT	https://hde.sit.oxisaas.com/OXiHDEServices/v1.0
UAT	https://hde.uat.oxisaas.com/OXiHDEServices/v1.0
PROD	https://hde.oxisaas.com/OXiHDEServices/v1.0

5. MIME Interface

As with the EDIaaS HDE SOAP web service, refer to the previously mentioned ACA documentation for a specification of the MIME interface. The EDIaaS HDE MIME service implements the same set of ACA operations as the EDIaaS HDE web service. There is no MIME changePassword equivalent. Trading partners that consume the MIME service must use the above SOAP changePassword operation to change the security password.

The table below lists the EDIaaS HDE MIME service web application URL's.

Table 3 – EDIAAS HDE MIME URL's

Env	Endpoint
SIT	https://hde.sit.oxisaas.com/OXiHDEServicesMIME/v1.0
UAT	https://hde.uat.oxisaas.com/OXiHDEServicesMIME/v1.0
PROD	https://hde.oxisaas.com/OXiHDEServicesMIME/v1.0

6. Contact Information

EDI Helpdesk: 1-800-933-6593, option 4

Email: ksxix-edikmap@gainwelltechnologies.com

Please have your applicable Trading Partner ID available before you call in order to minimize the amount of time needed to address your issue.

Contact KMAP Customer Service instead of EDI if you have questions regarding the details of a member's benefits, claim status information, or other services. Customer Service is available at 800-933-6593, option 6 (Monday – Friday 8 AM to 5 PM CST)

Note: Please have your applicable provider number available before you call in order to minimize the amount of time needed to address your issue.

7. Change Summary

Version Number	Date Modified	Modified By	Sections impacted
1.0	11/16/2014	Scott Medling	Initial Creation
2.0	11/02/2015	Wendy Long	HPE Updates
3.0	05/17/2021	Kevin Welch	GWT company name and logo updates.
4.0	12/6/2022	Kevin Welch	Added EDIaaS interface information to sections 4 and 5