

DATS

Development Applications and Technical Services

Centers for Medicare & Medicaid Services



Centers for Medicare & Medicaid Services
Financial Management
Systems Group
7500 Security Blvd
Baltimore, MD 21244-1850

Implementation Guide For Health Information Handlers (HIHs)

Electronic Submission of Medical Documentation System (esMD)



Version: 8.6 Final

Last Modified: 06/28/2016

Document Number: HIH_Implementation_Guide
Contract Number: HHSM-500-2015-00146U

Approvals

Signature: _____ Date: 07/06/2016

Print Name: Maureen Hoppa

Title: Contracting Officer's Representative

Role: CMS Approving Authority

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
8.6	06/28/2016	Vijayalakshmi Muthukrishnan, DATS	Resolved CMS comments for Version 8.5
8.5	06/10/2016	Vijayalakshmi Muthukrishnan, DATS	Resolved CMS comments for Version 8.4
8.4	05/23/2016	Vijayalakshmi Muthukrishnan, DATS	Resolved CMS comments for version 8.3
8.3	05/16/2016	Vijayalakshmi Muthukrishnan, DATS	Resolved CMS comments for version 8.2
8.2	04/28/2016	Vijayalakshmi Muthukrishnan, DATS	Updated for Release AR2016.07.0
8.1	03/09/2016	Vijayalakshmi Muthukrishnan, DATS	Resolved CMS comments.
8.0	02/05/2016	Justin Nelson, TOSS Jim Runser, DATS	Updated payload size for Release AR2016.03.0.
7.9	08/07/2015	Vijayalakshmi Muthukrishnan	Incorporated esMD_R_4_1_HIHImplementationGuide_v_7_8_Comments
7.8	07/24/2015	Vijayalakshmi Muthukrishnan	CMS' HIH Implementation Guide, version 7.6 comments, have been incorporated in this version.
7.7	07/16/2015	Vijayalakshmi Muthukrishnan	Updated the esMDCaseld attribute and added a note about the Sender ID and Receiver ID.
7.6	6/18/2015	John Dondapati	URLs have been updated, where applicable, and new Appendix G have been incorporated.
7.5	3/27/2015	Ed Klein	Updated regarding ADMC and ClaimID
7.4	03/27/2015	John Dondapati	Updated per CMS comments related to 7.3 version.
7.3	03/24/2015	John Dondapati	Updated per CMS comments related to 7.2 version.
7.2	03/13/2015	Shiva Velappan John Dondapati Srinivasarao Eadara Bindiya Vaishnav Aarti Nashte James Littlejohn	Restructured the document. Updated per CMS feedback.

Version	Date	Changed By	Items Changed Since Previous Version
7.1	02/20/2015	Shiva Velappan John Dondapati Srinivasarao Eadara Bindiya Vaishnav Aarti Nashte James Littlejohn	Restructured the document. Updated per CMS feedback.
7.0	01/08/2015	Murugaraj Kandaswamy Srinivasarao Eadara John Dondapati Melony Stehlik	Added the Section 10. CAQH Profile in Updated the Section 11. PA Review Responses with Release 4.0 responses Added the Section 12. Administrative Error Response Added the Appendix H Fixed all the Appendices with the right formatting.
6.3	12/05/2014	Melony Stehlik	Updated Table 7; added RRB OID.
6.2	10/01/2014	Melony Stehlik	Updated Table 6 Heading for PMD PA to PA Requests. Updated the following error codes in Table 19: ESMD_321 and ESMD_322 to adequately address the new Prior Authorization lines of business. Updated for Section 508 compliance.
6.1	09/17/2014	Melony Stehlik	Updated guide according to CMS' comments.
6.0	08/27/2014	Melony Stehlik	Updates incorporated for Release 3.1. Updated Table 5; added Claim ID optional for Appeals, Recommended the use of the standard format, as opposed to the composite format, added Non-Emergent Ambulance Transport PA requests and Hyperbaric Oxygen PA requests. Updated Table 6; added new lines of business. Updated Table 9; added new lines of business. Updated Table 14; added new lines of business.
5.3	8/15/2014	Melony Stehlik	Updated Table 7 with OIDs for AdvanceMed, ZPIC Zones 2 and 5 Updated references to EFT to CMS Enterprise File Transfer system in the system notification messages
5.2	5/12/2014	Melony Stehlik	Updated Figure 4 and section 8.5.2.

Version	Date	Changed By	Items Changed Since Previous Version
5.1	5/08/2014	Melony Stehlik	Removed three columns from Table 7.
5.0	4/26/2014	Melony Stehlik	Updated Introduction Updated Links
4.9	4/24/2014	Melony Stehlik	Updated Table of Contents Updated List of Tables Updated Table 1 to remove future specifications. Updated Table 5 Updated Table 7, removed PWK reference, and added new use cases. Updated Note below Table. Updated Table 14 to clarify title Updated Table 15 Added Virus Scan in Validations and removed PWK reference. Removed PWK Reference and added three new lines of business in section 8.2. Updated Figure 4 Updated Glossary; removed PWK Updated references to EFT to CMS Enterprise File Transfer system Updated Appendix F to indicate the change of the file size limitation from 19MB to 50MB.
4.8	4/18/2014	Melony Stehlik	Updated pg. 32, CONNECT 3.1 to 4.2 Updated diagrams Updated section 8 5.4 Updated pg. 86 ECM to EFT
4.7	4/17/2014	Melony Stehlik	Updated Table of Content Updated Introduction Updated Figure 1 Removed all references to PWK in Table 5 and Table 9 Updated Tables 17 and 19; Error Messages and Sample Error Messages Updated Table 14 with new use case Content Type Codes and descriptions Updated Table 15 Updated Appendix C
4.6	11/19/2013	Loren Adams	Removed PWK as an Inbound Use Case Response (Page 95); and Updated from CONNECT 3.1 to CONNECT 4.2 and include the Application Server: WAS 7.0 (Page 95)

Version	Date	Changed By	Items Changed Since Previous Version
4.5	10/23/2013	Laura Higdon	Updated Table 7 – Intended Recipient Table – Deleted MAC J14 (transitioned to MAC JK) and associated footnote. Added ZPIC Zone 4 OID to the Table.
4.4	10/11/2013	Laura Higdon	Updated Table 7 – Intended Recipient Table: Deleted MAC J1 and MAC JE footnote. Added MAC J14 footnote. Amended note under Table 7 regarding DME MACs accepting PA PMD (added all MACs). Updated Note under Table 9 regarding LOBs – removed release specific reference. Appendix G: Deleted PMD reason codes – PMD3O, PMD3P, and PMD3V. Added PMD reason codes – PMD2R, PMD2S, PMD2T, PMD4Q, PMD7G, PMD7H, PMD7I, PMD8E
4.3	09/04/2013	Theresa Howard	Changed Project to System on Cover Formatted: Table 7, section 17.1.1.2 Updated language in Sections: 10.1, 10.2, 10.3, 10:4, 10.6, 10.6.1, 10.6.2, 10.6.5, 10.6.6, 11, 12, 13, 14, 15, 17 Updated Table 7 – added ZPIC Z3 OID; replaced MAC J12 with MAC JL; replaced MAC J13 with MAC JK. Removed Appendix H – HIH Onboarding Prerequisites Removed Appendix H reference to Section 2.1
4.2	07/18/2013	Laura Higdon	Updated PMD Reason Identifier descriptions in Appendix G for PMD Reason Identifiers: PMD3A, PMD3C, PMD3G, PMD3K, PMD3M, PMD3N, PMD3Q, PMD3S, PMD4J, PMD5C, PMD5D, PMD7C, PMD7D, PMD9D, and PMD9G. Added Appendix H – HIH Onboarding Prerequisites Added Appendix H reference to Section 2.1 Updated PMD Reason Identifier descriptions in Appendix G for PMD Reason Identifiers: PMD1Z, PMD2Q, PMD2Z, PMD3Z, PMD4Z, PMD5Z, PMD6Z, PMD7Z, PMD8Z, and PMD9Z. Updated Table 7 – replaced Title 18 with MAC J6

Version	Date	Changed By	Items Changed Since Previous Version
4.1	06/14/2013	S. Girde	<p>Updated the PMD Reason Identifier description in Appendix G for the PMD Reason Identifiers: PMD1Z, PMD2Z, PMD3Z, PMD4Z, PMD5Z, PMD6Z, PMD7Z, PMD8Z & PMD9Z</p> <p>Table 21, Section 10.3, Table 22, Section 10.4 and Section 10.6.4: Updated the language to reflect that the PMD Reason Identifier Description shall not be sent for PMD Reason Identifiers: PMD1Z, PMD2Z, PMD3Z, PMD4Z, PMD5Z, PMD6Z, PMD7Z, PMD8Z & PMD9Z</p>
4.0	05/3/2013	Sacchidanand Girde, Laura Higdon, Vasanth Kalakota, Sumit Kapoor, S. Eadara, V. Gopalakrishnan	<p>Added Section 10 for PMD PA Outbound. Revised Section 11: Release Notification Details.</p> <p>Added Appendix G: PMD Reason Identifier and Statements.</p> <p>Table 19: Changed the language of the error messages for PMD PA inbound requests to be PMD PA specific.</p> <p>Table 19: Moved the error message sent to the HIHs for submitting payloads > 19 MB under First Notification Errors.</p> <p>Updated Sections 1 and 2.</p> <p>Added Payload Check to Section 6.</p> <p>Updated Figure 1.</p> <p>Removed NHIN, as necessary.</p> <p>Added eHealth Exchange were necessary.</p> <p>Updated Intended Recipient Table 7.</p> <p>Table 9 and Table 14: Removed Content Type Codes for lines of business not included in esMD Production (PROD).</p>
0.1	Will research date and update in a future version.	Melanie Combs-Dyer	<p>Initial Draft (Of note – hereafter, the Document Change History table will only include information that reflect document changes beginning at Version 4.0 until present. History of document changes prior to Version 4.0 can be located on previously approved esMD Implementation Guides versioned 3.9 or earlier.</p>

Table of Contents

1	Introduction	15
1.1	The esMD Overview	15
1.2	Overview of Medicare Claim Review Programs	15
1.2.1	Claim Review Contractors	16
1.2.2	Claim Review Programs.....	16
1.3	Overview of the esMD Processes	16
1.3.1	Previous esMD Process	16
1.3.2	Current esMD Process	17
1.4	The esMD Primary Audiences	18
1.4.1	Important Note on the Onboarding Process for HIHs.....	19
2	The esMD Onboarding Process for HIHs	20
2.1	The esMD Onboarding Instructions for Prospective HIHs	20
2.1.1	The esMD Gateway Environment Testing and Configuration	20
2.1.2	Health Level 7 Organizational Identifiers (OIDs).....	20
2.1.3	Obtaining an HL7 OID	20
2.1.4	HIH Gateway Internet Protocol (IP) Address	20
2.1.5	HIH Gateway Endpoint Uniform Resource Locator (URL) for Responses	21
2.1.6	Transport Layer Security (TLS) Certificate	21
2.1.7	Federal Information Processing Standards (FIPS) for Cryptographic Modules.....	22
2.1.8	X12 Specific Information.....	22
2.1.9	Completion of Onboarding process.....	22
2.2	HIHs Suspending Participation before Completing Onboarding Process ...	22
2.3	Temporary or Permanent Access Removal (Offboarding an HIH)	22
3	HIH Technical Requirements for Submitting and Transmitting Documentation	23
3.1	Mandatory HIH Completion of Integration and the esMD Interoperability Testing.....	23
3.2	CMS Validation Region Testing with HIH.....	23
3.3	CMS Production Region Connectivity Verification with HIH	23
4	The esMD System Profiles.....	25
4.1	The esMD System XDR Profile.....	25
4.2	The esMD System CAQH Profile	25

5	XDR Interface Definition	26
5.1	Interface Descriptive Name	26
5.2	Interface Level	26
5.3	Definition	26
5.3.1	Interaction Behavior	26
5.3.2	Triggers	28
5.3.3	Transaction Standard	28
5.3.4	Technical Pre-Conditions	28
5.3.5	SOAP Message Envelope	29
5.3.6	SAML Assertions	30
5.3.7	Assertions Design Principals and Assumptions	31
5.3.8	Assertions Transaction Standard	31
5.3.9	Specific Assertions	31
5.3.10	The esMD SAML Assertion Details	32
5.3.11	SAML Assertion Attributes	41
5.3.12	Version Attribute	41
5.3.13	ID Attribute	41
5.3.14	Issue Instant	41
5.3.15	Issuer	41
5.3.16	Subject	41
5.3.17	SAML Statement Elements	41
5.3.18	Attribute Statement	41
5.3.19	Subject ID Attribute	41
5.3.20	Home Community ID Attribute	42
5.3.21	Purpose of Use Attribute	42
5.3.22	National Provider Identifier (NPI) Attribute	42
5.3.23	Intended Recipients Attribute	42
5.3.24	Authentication Statement	43
5.3.25	Authentication Method (AuthnContext)	43
5.3.26	Subject Locality	43
5.3.27	Authentication Instant (AuthnInstant)	43
5.3.28	Session Index	43
5.3.29	Example	43
5.3.30	Authorization Decision Statement	43
5.3.31	Action	44
5.3.32	Decision	44

5.3.33 Resource	44
5.3.34 Evidence.....	44
5.3.35 Assertions.....	44
5.3.36 Target Communities	45
5.3.37 Metadata Fields	45
5.3.38 The esMD Functional Specific Submission Set Metadata Attributes	46
5.3.39 Attachment Control Number (ACN).....	93
5.3.40 Intended Recipients.....	93
5.3.41 Content Type Code.....	93
5.3.42 HITSP C62 (Construct on Top of CDA) Document Constraints.....	100
5.4 Content Type Codes	109
6 XDR Validation	111
7 XDR Error Messages	112
8 XDR Status and Notification Messages	114
8.1 The esMD First Acknowledgment - HTTP Status Code	114
8.1.1 Success Message.....	115
8.1.2 The esMD Error Messages	116
8.2 The esMD System First Notification	118
8.2.1 Metadata Validation	118
8.3 The esMD System Second Notification	129
8.3.1 Claim Review Pickup Status Notification.....	129
8.3.2 Claim Review Pickup Error Notification	131
8.4 The esMD System Third Notification	132
8.4.1 PA Review Response	132
8.4.2 PA Review Error Response	132
8.4.3 Review Contractor Administrative Error Notification	132
8.5 Information Contained in Response Message.....	134
8.5.1 Message ID (Correlated with Request MessageID).....	134
8.5.2 Unique ID (Correlated with Request UniqueID).....	134
8.5.3 RequestID.....	134
8.5.4 Status.....	135
8.5.5 Response Slots	136
8.5.6 Delivery to the CMS Enterprise File Transfer System (First Notification)	137
9 The esMD System CAQH Profile.....	138

9.1	Request Layout.....	138
9.2	CAQH CORE Real-Time Mode (Synchronous) and CAQH CORE Generic Batch Mode (Deferred) Messaging	138
9.3	HIH to the esMD - CAQH PA Request (Real Time).....	139
	9.3.1 Traceability Between Requests and Responses	140
	9.3.2 X12N 278 5010 Acknowledgements	141
9.4	The esMD X12N 278 5010 PA Request with XDR Additional Documentation	142
9.5	The esMD to HIH - CAQH PA Review Result Response (Batch Mode)	144
9.6	CAQH Metadata	146
9.7	Error Handling.....	149
9.8	CONNECT SAML Assertions	149
9.9	X12N 278 5010 Companion Guide	149
10	XDR PA Response.....	150
10.1	Overview	150
10.2	XDR PA Review Results Response.....	150
	10.2.1 XDR Review Response Data Elements	150
10.3	Rules about Situational Data Elements in the PA Review Results Response	152
	10.3.1 Situational Data Elements for Affirmed Decision	152
	10.3.2 Situational Data Elements for Non-Affirmed Decision	153
	10.3.3 Situational Data Elements for Modified Decision	153
	10.3.4 Situational Data Elements for Rejected Decision	154
10.4	Note on Reason Identifier (DEN Code).....	154
10.5	Rules about Unique Tracking Number in PA Review Results Response....	154
10.6	Status and Notification Messages for PA	155
10.7	Information Contained in the PA Review Results Response for XDR.....	156
	10.7.1 MessageID (Shall be Correlated with PA Request Message ID).....	156
	10.7.2 UniqueID (Shall Be Correlated with PA Request Unique ID)	157
	10.7.3 RequestID	157
	10.7.4 Status.....	158
	10.7.5 Response Slots	158
10.8	Sample Outbound PA Review Results Responses for XDR.....	161
	10.8.1 Affirmed PA Review Results Response.....	161
	10.8.2 Non-Affirmed PA Review Results Response	162
	10.8.3 The esMD Modified PA Review Results Response.....	164

10.8.4	The esMD Rejected PA Review Results Response	165
11	X12N 278 5010 PA Response	168
11.1	X12N 278 5010 Review Response Data Elements	168
11.2	X12N 278 5010 Error Response Data Elements	168
12	Retry Functionality	169
12.1	Retry Scenarios Common for Both X12 and XDR Transmissions.....	169
12.2	X12 Retry Scenarios	170
13	The esMD Reports to HIH.....	172
14	GLOSSARY	175
15	ACRONYMS	180
Appendix A.	SOAP Message For Inbound (HIH To CMS) Submissions.....	183
Appendix B.	C62 Payload Sample.....	194
Appendix C.	Test Types for HIHs.....	198
C.1	Connectivity Test in the Validation Environment.....	198
C.2	Testing Inbound Connection (HIH Gateway to the esMD Gateway)	198
C.3	Inbound Telnet Test.....	198
C.4	HIH Mutual TLS Certificate Authentication.....	199
C.5	Confirmation of Metadata Validation and Request Processing.....	200
C.6	Confirmation of Metadata Persistence in the esMD Database.....	200
C.7	Testing Outbound Connection (esMD Gateway to HIH Gateway).....	200
C.8	Outbound Telnet Test	200
C.9	Confirmation of Receiving the First Notification	201
C.10	Functionality Testing in the Validation Environment (Testing with the HIH Gateway Application)	201
C.11	Inbound Tests (HIH to the esMD Gateway).....	202
C.12	Validate Metadata and Request Processing	202
C.13	Metadata Persistence in the esMD Database	202
C.14	Delivery to the CMS Enterprise File Transfer System	202
C.15	Outbound Tests (HIH to the esMD Gateway)	202
C.16	End-to-End Testing in the Validation Environment (Testing with HIH Gateway Application and Not SOAP UI)	202
C.17	Testing with an Review Contractor	203
C.18	Receipt of Second Notification (Review Contractor Pickup).....	203

C.19	Connectivity Test in the Production Environment	203
C.20	End-to-End Testing in the Production Environment	203
Appendix D.	SOAP UI Configuration	204
D.1	Download and Initial Configuration	204
D.2	Test Execution	204
Appendix E.	Submission Guidelines for Certified HIHs	206
Appendix F.	Submitting Transactions with CONNECT Version 3.1, or Older Versions	207
Appendix G.	PA Reason Identifiers and Statements	208
Appendix H.	References	209
Appendix I.	The esMD Sample CAQH Real-Time Request	213

List of Tables

Table 1:	Medicare Prepayment and Post Payment Claim Review Programs	16
Table 2:	Name Spaces Details with CONNECT Software	30
Table 3:	Standard SAML Assertions in SOAP Envelope	31
Table 4:	The esMD SAML Assertion Details	33
Table 5:	The esMD Functional Specific Submission Set Metadata Attributes	48
Table 6:	The esMD Document Metadata Attributes	70
Table 7:	ClassCodes and Corresponding ClassCode Display Names	94
Table 8:	Content Type Codes and Corresponding Content Type Code Display Names	94
Table 9:	Confidentiality Codes	95
Table 10:	HealthCare Facility Type Code	96
Table 11:	Submission Set/Document Title	96
Table 12:	Document Format Code and Payload Type	96
Table 13:	Overall Mapping of Document Submission with Class and Content Type Codes ..	97
Table 14:	Combination of the esMD Codes and Claim/Case IDs for Different Types of Submission Requests	98
Table 15:	CDA Document Constraints Specifications	102
Table 16:	Content Type Code Descriptions	110
Table 17:	Error Messages	112
Table 18:	HTTP Status Codes	115
Table 19:	Sample Error Message Content	122
Table 20:	Possible Request Types	134
Table 21:	CORE Envelope Metadata	147
Table 22:	PA Review Results Response Data Elements for XDR	150

Table 23: Affirmed PA Review Results Responses	152
Table 24: Non-Affirmed PA Review Results Responses.....	153
Table 25: Modified PA Review Results Responses	153
Table 26: Rejected PA Review Results Responses	154
Table 27: UTNs in PA Review Results Responses	154
Table 28: PA Outbound Request Type	157
Table 29: Retry Scenarios Common for Both X12 and XDR Transmissions.....	169
Table 30: Retry Scenarios for X12 Transmissions Only.....	171
Table 31: HIH Daily Transaction Report in PDF format	173
Table 32: HIH Daily Transaction Report in Excel Format.....	174

List of Figures

Figure 1: Current esMD Process.....	17
Figure 2: Asynchronous Acknowledgments with Multiple Hyper Text Transfer Protocol (HTTP) Connections.....	27
Figure 3: SOAP Envelope with XDR Interchange/HITSP C62 Construct	29
Figure 4: Document Submission Deferred Responses with Multiple HTTP Connections ...	114
Figure 5: ASC X12N 278 5010 over CONNECT (CAQH CORE 270)	138
Figure 6: X12 PA Request in CAQH Real Mode	139
Figure 7: X12N 278 5010 Acknowledgements	141
Figure 8: X12N 278 5010 PA Request with Additional XDR Documentation.....	142
Figure 9: X12 PA Review Result Response in CAQH Batch Mode	145
Figure 10: Outbound Response Notification	155

1 Introduction

The Centers for Medicare & Medicaid Services (CMS) is a federal agency that ensures health care coverage for more than 100 million Americans. The CMS administers Medicare and provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs and Children's Health Insurance Program (CHIP). The CMS works together with the CMS community and organizations in delivering improved and better coordinated care.

1.1 The esMD Overview

Each year, the Medicare Fee-For-Service (FFS) Program makes billions of dollars in estimated improper payments. The CMS employs several types of Review Contractors (RCs) to measure, prevent, identify, and correct these improper payments. RCs find improper payments and manually review claims against medical documentation obtained to verify the providers' compliance with Medicare rules. The RCs request medical documentation by sending a paper letter to the provider. In the past, medical documentation providers had only two options for delivering the medical documentation requested by sending it by letter or fax.

The Electronic Submission of Medical Documentation (esMD) system gives providers the option of sending medical documentation electronically to a requesting RC, instead of sending the documentation by letter or fax.

Many providers use a Health Information Handler (HIH) organization to perform tasks, such as submitting claims and providing electronic health record systems. Any organization that handles health information on behalf of a provider is an HIH. Some HIHs are beginning to offer esMD gateway services, often referred to as Claim Clearinghouses, Release of Information vendors, Health Information Exchanges, and Electronic Health Record vendors.

The esMD allows providers, HIHs, and gateway services to send responses for requests for additional documentation electronically to a RC during the claims review process.

Currently, electronic medical documentation can be sent, using the esMD, in either in a Portable Document Format (PDF) or Extensible Markup Language (XML).

On September 15, 2011, the esMD allowed providers to be able to send medical documentation to RCs electronically and allowed providers to be able to receive a Prior Authorization Review Response from RCs.

The esMD utilizes and leverages web services, as a central source for providing greater interoperability, connectivity, and compatibility between providers, HIHs, and gateway services and is based on standards developed by the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology.

1.2 Overview of Medicare Claim Review Programs

The CMS implemented several initiatives to prevent improper payments before CMS processes a claim, and to identify and recover improper payments after processing a claim. The overall goal is to reduce improper payments by identifying and addressing coverage and coding billing errors. The Government estimates that about 8.5 percent of all Medicare FFS claim payments are improper. (For the most current information, visit <http://www.paymentaccuracy.gov/programs/medicare-fee-service>).

1.2.1 Claim Review Contractors

Under the authority of the Social Security Act, CMS employs a variety of contractors to process and review claims in accordance with Medicare rules and regulations. Please refer to the following link for more information on the esMD Review Contractors:

http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which_Review_Contractors_Accept_esMD_Transactions.html

1.2.2 Claim Review Programs

This implementation guide describes five claim review programs and their roles in the life cycle of Medicare claims processing. Each claim review program has a level of review: complex or non-complex. Non-complex reviews do not require a clinical review of medical documentation. Complex reviews require licensed professionals who review additional requested documentation associated with a claim.

Table 1: Medicare Prepayment and Post Payment Claim Review Programs lists the prepayment and Post Payment Claim Review Programs referenced in this implementation guide.

The columns in Table 1: Medicare Prepayment and Post Payment Claim Review Programs divide the Medicare claim review programs based on performance of prepayment or Post Payment reviews. Prepayment reviews occur prior to payment. Post Payment reviews occur after payment. The Medical Review (MR) Program can perform both prepayment and Post Payment reviews.

Table 1: Medicare Prepayment and Post Payment Claim Review Programs

Prepayment Claim Review Programs*	Post Payment Claim Review Programs
National Correct Coding Initiative (NCCI) Edits	Comprehensive Error Rate Testing (CERT) Program
Medically Unlikely Edits (MUEs)	Recovery Audit Program
Medical Review (MR)	Medical Review (MR)

In 2012, CMS introduced the Recovery Audit Prepayment Review Demonstration, which allows Recovery Auditors to conduct prepayment reviews on certain types of claims that historically result in high rates of improper payments. The demonstration focuses on 11 States: California, Florida, Illinois, Louisiana, Michigan, Missouri, New York, North Carolina, Ohio, Pennsylvania, and Texas.

1.3 Overview of the esMD Processes

1.3.1 Previous esMD Process

In the past, RCs sent a notification and medical documentation request letter to inform providers that they have been selected for a review and that the RC is requesting the provider to provide specific medical documentation in order for the review to be completed.

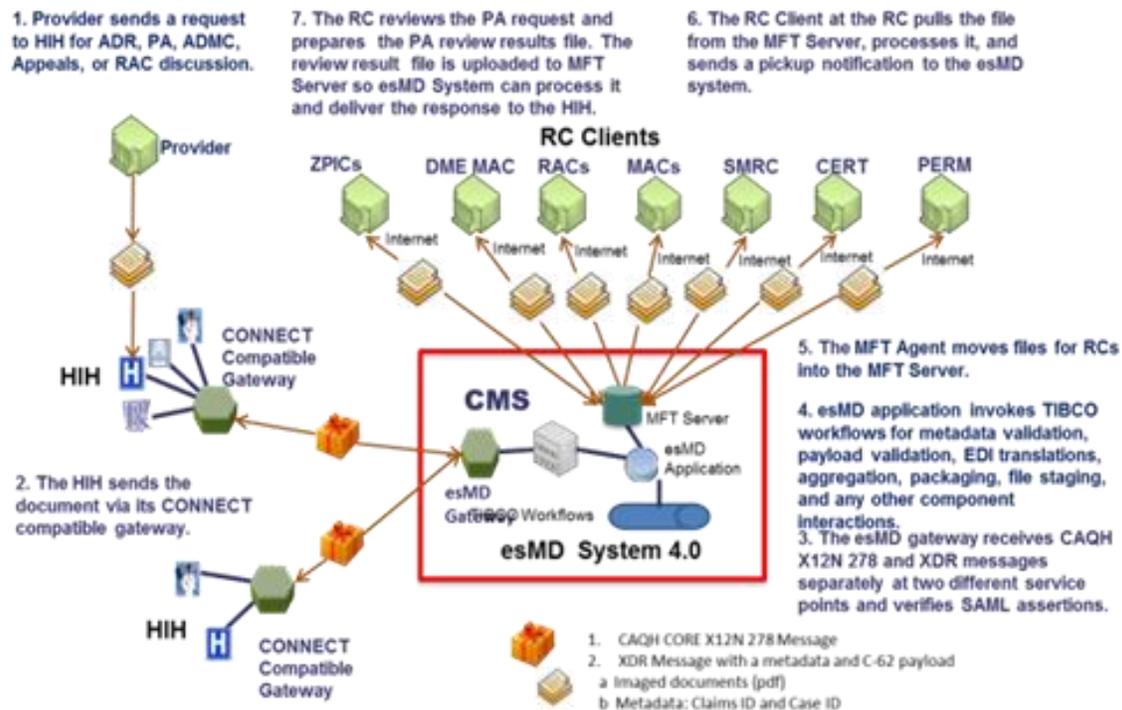
A provider could send the medical documentation to the RC in three ways: mail the requested documentation to the RC, mail a Compact Disc (CD) containing the medical documentation in a PDF or Tagged Image File Format (TIFF) file, or transmit the documentation using a fax machine.

1.3.2 Current esMD Process

1. With the current esMD system that is available for providers, HIHs, and RCs, these organizations now have a fourth choice. The esMD system allows providers to electronically send a response back in answer to the ADR letter, to RCs, saving time, postage, and reducing paperwork, who have successfully completed the CMS esMD Onboarding
2. In addition, the esMD system allowed providers with an electronic way of submitting Prior Authorization (PA) requests to Durable Medical Equipment (DME) Medicare Administrative Contractors (MACs), starting in January 2013.
3. The esMD system enabled providers to submit First Level Appeals Request, Recovery Auditors Discussion Requests, and Advanced Determination of Medical Coverage (ADMC) Requests with the Release 3.0 (July 2014).
4. The esMD system enabled providers to submit the following two new Prior Authorization (PA) Requests with Release 3.1 (October 2014): Non-emergent Hyperbaric Oxygen (HBO); and
5. Repetitive Scheduled Non-Emergent Ambulance Transport (Ambulance) to RCs with the Implementation of Release 3.1 (October 2014).

Figure 1: Current esMD Process illustrates the current esMD process.

Figure 1: Current esMD Process



The esMD Release 4.0 (R4.0) was implemented in June 2015 and focused on the Electronic Data Interchange (EDI) between Health Information Handlers (HIHs) and the esMD. The esMD Release 4.0 introduced the EDI ASC X12N 278 5010 file format for submitting all PA requests. In addition to the above, the esMD R4.0 is utilizing existing Cross-Enterprise Document Reliable Interchange (XDR) profile to submit all PA programs and other Lines of Business. The following list describes the PA programs and other Lines of Business:

1. PA programs: PMD, HBO, Ambulance, and Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS)
2. First Level Appeal Requests;
3. RA Discussion requests;
4. ADMC requests; and
5. Responses to Additional Documentation Requests (ADRs).

Note: The Programs , Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) and the Pre-Claim Review Demonstration for Home Health Services will accept only X12 requests. The Pre-Claim Review Demonstration for Home Health Services is hereafter referred to as "HPCR."

The esMD Release AR2016.07.0 will be implemented in July 2016 and will include the following programs.

1. Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS),
2. HPCR Demonstration requests

Note: These above two programs only support EDI format (X12N 278).

3. Second level Appeal Requests.

The following provides an overview of the steps in the process.

1. **The provider decides what to submit.** In both the current paper process and the new the esMD process, the RC does not specify which documents the provider must send. It is up to the provider to decide which documents to send. The documents that a provider may submit include discharge summaries, progress notes, orders, radiology reports, lab results, etc.
2. **The initial phase of the esMD allows only unstructured documents. The esMD only accepts unstructured documents in PDF files.**
3. **Provider to RC Documentation Submission and PA Review Responses only.** Phase 1 of the esMD includes electronic document submission (from provider to RC) and PA Review Responses (from RC to provider) only. It does not include the Electronic Medical Documentation Request (eMDR) from RC to provider.
4. **Each package must contain documentation about a single claim of a beneficiary.** Throughout this profile, the term "package" will be used to refer to one (1) or more documents associated with a single beneficiary. Each package can contain multiple documents, as long as all documents relate to the same claim of a beneficiary. The technical term for a package is a Simple Object Access Protocol (SOAP) message.
Note: More details about the esMD data exchange can be found in the esMD Profile. Refer to <http://exchange-specifications.wikispaces.com/esMD+Profile+Definition>.
5. **The CMS is not involved in the business relationship between the Health Information Handler (HIH) and the provider.** This document does not describe how HIHs should collect or store medical documentation from the providers. The HIH and provider must comply with all applicable Health Information Portability and Accountability Act (HIPAA) provisions.

1.4 The esMD Primary Audiences

The primary audience for this document includes HIHs such as Regional Health Information Organizations (RHIOs), Health Information Exchanges (HIEs), Release of Information (ROI) vendors,

claim clearinghouses, and other organizations that securely submit medical documentation on behalf of providers via CONNECT compatible gateways to RCs.

Note: This implementation guide refers to RHIOs, HIEs, ROI vendors, claim clearinghouses, and other entities that move health information over secure CONNECT compatible gateways on behalf of health care providers as HIHs.

HIHs who have built a CONNECT compatible gateway and wish to submit through the esMD system, please follow the instructions provided at this link: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Information_for_HIHs.html.

For more information about CONNECT Gateways, refer to www.connectopensource.org. For a list of HIHs that currently participate in the CMS esMD Program, refer to [http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which HIHs Plan to Offer Gateway Services to Providers.html](http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which_HIHs_Plan_to_Offer_Gateway_Services_to_Providers.html).

Another audience for this document includes the software developers who aim to assist RCs in viewing and more efficiently processing documents received in the esMD format. Software developers that develop products to assist HIHs in receiving data easily from a provider's Electronic Health Record (EHR) in the esMD format.

For additional information and related documents on the esMD processes and software, see Appendix H References.

1.4.1 Important Note on the Onboarding Process for HIHs

The esMD will only accept transmissions from organizations that have successfully completed the esMD Onboarding process. The HIH must sign the CMS esMD agreement for submitting X12 requests and to receive the unmasked PHI in the response from the esMD system.

2 The esMD Onboarding Process for HIHs

Note: The Onboarding process below applies to HIHs submitting both XDR and X12 transmissions.

2.1 The esMD Onboarding Instructions for Prospective HIHs

The HIH shall complete and submit the esMD HIH Onboarding Request Form, along with the results of successfully completed CONNECT/CONNECT-compatible self-tests to the esMD Support Team to the following email address: esMD_Support@cms.hhs.gov.

The HIH Onboarding Request Form is located on the following CMS Government website:

http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Information_for_HIHs.html. The following sections include additional information on the information that will be provided by an HIH on the HIH Onboarding Request Form.

2.1.1 The esMD Gateway Environment Testing and Configuration

The esMD Support Team will verify that the environment details that have been provided by the HIH are acceptable and will validate that the CONNECT/CONNECT-compatible self-tests conducted by the HIH were successful, based on the self-tests results submitted to the esMD Support Team.

Note: Any changes to any environment details, submitted in the HIH's HIH Onboarding Request Form, after the submission of the form to the esMD Support Team, could possibly cause a delay in testing.

2.1.2 Health Level 7 Organizational Identifiers (OIDs).

All Health Level 7 (HL7) OIDs will have a "2.16.840.1.113883." prefix.

The [joint-iso-itu-t(2) country(16) us(840) organization(1) hl7(113883).] will be followed by an OID Type (e.g., 2.16.840.1.113883.3.xxx.x).

The HIH will use the appropriate OID Type, based on their organization type and purpose.

Most HIHs will register, using their OIDs with an OID Type = "3 - Root" to be a Registration Authority with the esMD.

Note: External groups have been issued a specific "HL7 OID Root" that is appropriate for their use.

2.1.3 Obtaining an HL7 OID

An HIH may obtain a HL7 OID and find more information on obtaining an OID from the following Health Level 7 organization's website: www.hl7.org.

An HIH may register an OID obtained from the HL7 website on the following website: <http://www.hl7.org/oid/index.cfm>.

- Note: After going to the <http://www.hl7.org/oid/index.cfm> website, select the **Obtain or Register an OID** link on the top right corner to register an OID.

2.1.4 HIH Gateway Internet Protocol (IP) Address

1. The HIH is required to submit the HIH's IP address for the HIH's Gateway to the esMD Support Team.

Note: A "public-facing" IP Address is the IP address that identifies the HIH's network and allows the esMD Gateway to connect to the HIH's network from the Internet.

2. The HIH will hide their internal private IP address by using Network Address Translation (NAT) (known as, "NATing") for the HIH's public-facing IP address.
3. The HIH technical team will contact their network team to procure or assign a public-facing IP address to their internal private IP. (For example: A public-facing IP address can be purchased from AT&T, Verizon, etc.).
4. If an HIH is using multiple esMD servers, then the HIH will submit either "one" IP address for both inbound and outbound traffic; or submit "one" IP address for inbound transmissions and "another" IP address for outbound traffic.

Note: The esMD Support Team suggests that an HIH use load balancing and NATing to convert and submit a request from multiple servers to one IP address. The HIH can submit either one IP address for both inbound and outbound traffic; or, two IP addresses, one for inbound traffic and another one for outbound traffic, by submitting this information to the esMD Support Team on the HIH Environmental Details Form.

2.1.5 HIH Gateway Endpoint Uniform Resource Locator (URL) for Responses

An HIH is required to submit the URL for the HIH's Gateway Endpoint to receive responses from the esMD system to the esMD Support Team.

2.1.6 Transport Layer Security (TLS) Certificate

The HIH is required to obtain a server certificate from a Certificate Authority (CA), a trusted third party organization or company that issues digital certificates used to create digital signatures.

The HIH shall include the following sever certificate information in the HIH Onboarding Request Form submitted to the esMD Support Team:

- Server Certificate;
- Intermediate Certificates (if applicable); and
- Root Certificate.

All CAs must adhere to the following guidelines in order to be submitted to the esMD Support Team:

1. Level 2 Identity Proofing, as described in the National Institute of Standards and Technology (NIST) publication:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf> (Specifically, refer to Table 3 - Identity Proofing Requirements by Assurance Level, in the PDF, under section 5.3.1. General Requirements per Assurance Level.)
2. 2048 bit RSA keys
3. Advance Encryption Standard (AES) 128 bit encryption
4. Secure Hash Algorithm-2 (SHA-2, 256 bit at least) certificate signing algorithm since SHA-1 is being rapidly deprecated.
5. Server Level and server-to-server communication certificate. (**Note:** No wild card (*.*) or domain level certificate are accepted).

Note: HIHs should note the expiration date of their certificates and plan accordingly to renew and submit certificate renewals to the esMD Support Team four weeks in advance of the expiration date.

For more information, refer to:

- http://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf: Appendix B, SC13-1; and
- <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

2.1.7 Federal Information Processing Standards (FIPS) for Cryptographic Modules

All cryptographic modules used by HIH eHealth Exchange instances (typically CONNECT) must adhere to Federal Information Processing Standards (FIPS) 140-2 Compliance criteria and must have a TLS CA.

"FIPS 140-2" is a government standard that provides a benchmark on how to implement cryptographic software (<https://technet.microsoft.com/en-us/library/cc180745.aspx>).

For a CONNECT-based solution, this standard has to be followed to ensure that the CONNECT Gateway is FIPS 140-2 compliant. Any HIH that needs to communicate with the esMD Gateway needs to have the FIPS mode enabled.

2.1.8 X12 Specific Information

The HIH is required to provide the Sender ID that is included in an X12N 278 request to identify the HIH as part of the HIH Onboarding form. This is only required if the HIH is planning to submit X12N 278 requests.

2.1.9 Completion of Onboarding process

Upon successfully completing the onboarding process, the HIH will receive an e-mail notification from the esMD Support team that they have completed the onboarding process. The HIH will then be involved in integration and interoperability testing. The start of testing begins with sending the required claim documentation through the esMD Gateway for the Validation environment and later for the Production environment.

2.2 HIHs Suspending Participation before Completing Onboarding Process

HIHs, who suspend participation before they fully complete the onboarding process, will receive an esMD program Exit Letter from the esMD Support team.

2.3 Temporary or Permanent Access Removal (Offboarding an HIH)

CMS reserves the right to temporarily or permanently remove access for the HIH, if the HIH fails to meet the requirements and standards set forth in this document (refer to sections 5.3.3 Transaction Standard and 5.3.4 Technical Pre-Conditions); and, by doing so effectuates a technical disruption to the esMD application.

3 HIH Technical Requirements for Submitting and Transmitting Documentation

3.1 Mandatory HIH Completion of Integration and the esMD Interoperability Testing

Quick Overview: Before submitting documentation through the esMD system, the onboarding HIH is required to complete the Integration and the esMD Interoperability testing. This phase of testing requires the HIH to submit claim documentation through the esMD Gateway in the Validation environment.

Upon successful completion of the testing in the esMD Validation (VAL) region, HIHs will get an approval email from the esMD Support Team to proceed with testing in the esMD Production environment.

3.2 CMS Validation Region Testing with HIH

The esMD Support team shall provide the HIH with the Validation Configuration Document containing CMS' Environment Details. After the HIH successfully configures CMS' Environment details on their end, the HIH will begin testing through the esMD VAL CONNECT Gateway.

1. The esMD Support Team and the HIH perform the Connectivity test.
2. The esMD Support Team will coordinate the manual Interoperability and End-to-End integration testing between the esMD CONNECT Gateway and the HIH through email.
3. Troubleshooting calls shall be scheduled if there issues arise.
4. Upon successful completion of the Interoperability and Integration testing (i.e., transmission of 100% correctly formed payload and receipt of the two asynchronous responses back from the esMD system) between the HIH and the Validation environment. The HIH will officially receive an email notification from the esMD Support Team. The HIH will start Connectivity and Integration testing in the esMD Production environment.

3.3 CMS Production Region Connectivity Verification with HIH

All HIHs shall receive the esMD Production Configuration document prior to verification of connectivity to the esMD Production environment.

This verification is performed through the esMD Production CONNECT Gateway.

1. The HIH will configure its gateway with the esMD CONNECT Gateway PROD region OID 2.16.840.1.113883.13.34.110.1.
2. The esMD Support team and the HIH shall perform the connectivity verification.
3. The esMD Support team will coordinate the verification task by opening a conference call with the related stakeholders and sharing the results. A manual process will be performed, due to the lack of automated XDR tools.
4. Upon successful Connectivity and Integration verification (i.e., transmission of 100% correctly formed payload and receipt of the two asynchronous responses back from the esMD Gateway) between the HIH and the CMS Production esMD Gateway, the HIH

will officially receive communication from the esMD Support team they may officially transmit the claim documents through the Production esMD CONNECT Gateway.

4 The esMD System Profiles

4.1 The esMD System XDR Profile

This esMD Implementation Guide provides more information about the transmissions sent using the esMD XDR at the following link: http://exchange-specifications.wikispaces.com/file/view/ESMD_XDR_Production_Specification_v1.0.pdf.

4.2 The esMD System CAQH Profile

The esMD X12 Document Submission Service Specification provides more information about the CAQH Profile at the following link http://exchange-specifications.wikispaces.com/file/view/CAQH%20CORE%20X12_DocumentSubmissionServiceSpecification%20v1.0.doc.

5 XDR Interface Definition

5.1 Interface Descriptive Name

The HIH adopts the IHE XDR profile in a SOAP envelope with ITI – 41 Provide and Register Document set – b transaction metadata and C62 document payload attachment. Each SOAP message can contain multiple document attachments related to the same claim of a patient. As of Release AR2016.03.0, the esMD allows the HIH to submit messages up to 200 MB in size. The esMD Gateway allows the HIH to submit multiple SOAP messages with different Unique IDs for a Claim Document Request of a patient.

5.2 Interface Level

The XDR interface level includes XDRs transmitted to and from the HIHs to the esMD CONNECT Gateway.

5.3 Definition

5.3.1 Interaction Behavior

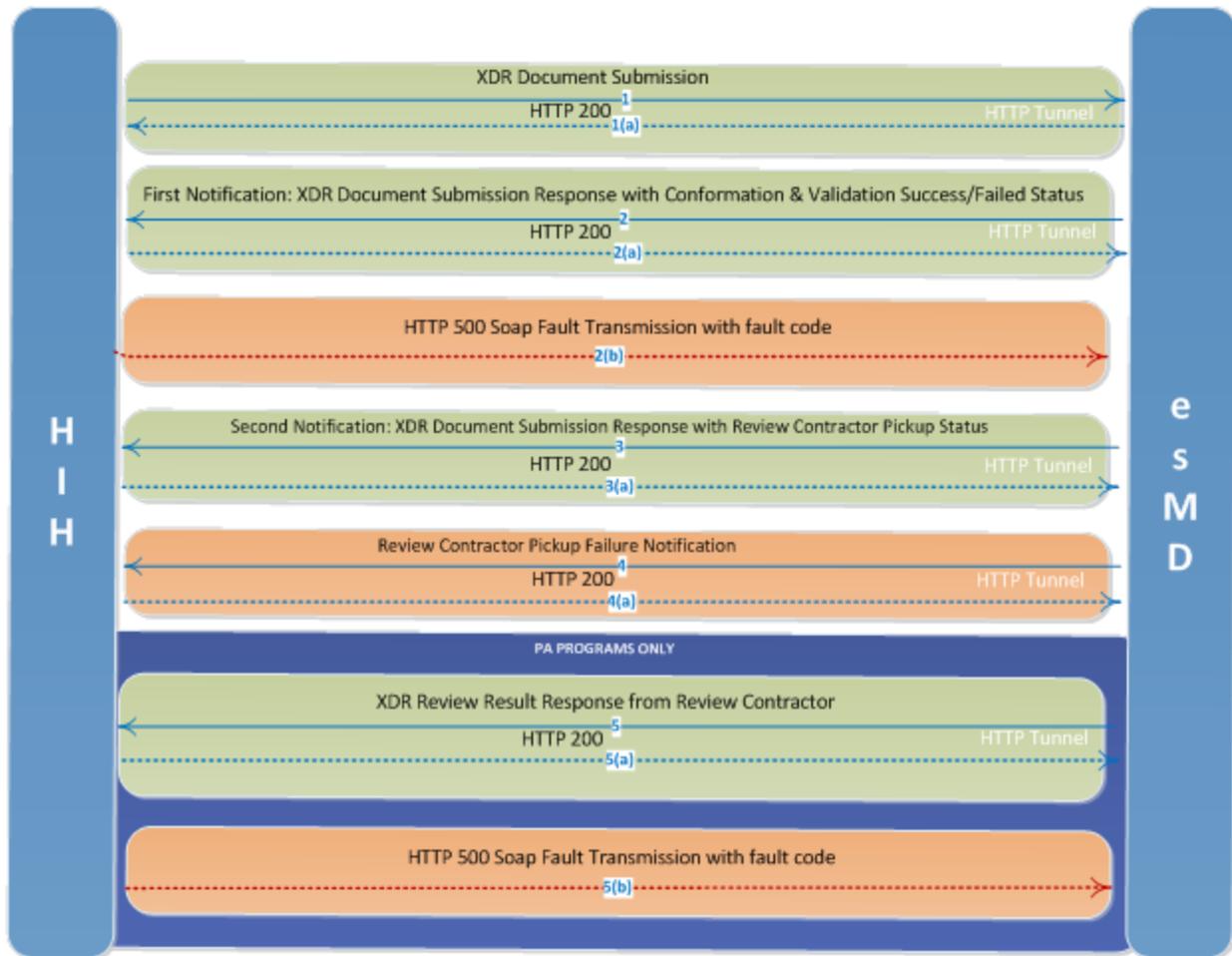
Figure 2: Asynchronous Acknowledgments with Multiple Hyper Text Transfer Protocol (HTTP) Connections illustrates the communication between the HIH and the esMD CONNECT Gateway with asynchronous messaging with three HTTPS requests.

The HIH Gateway submits the electronic medical claim documentation, based on the CMS onboarded HIH and their gateway OID. The HIH submits the IHE XDR profile SOAP Messages to the CMS with the ITI – 41 (Provide and Register Document Set – b) transaction, SAML Assertions, Document Submission Meta Data, and C62 Payload in the SOAP body.

The esMD CONNECT Gateway receives the request, with SAML Assertions, and consults its gateway Policy Enforcement Point (which could be a SAML authority) which, in turn, uses the esMD database to establish whether the submitted Home Community ID will be allowed to perform the esMD document submission function.

Assertions can convey information about the authentication and authorization acts that the HIH performed by subjects (the OID acts as a User ID), its attributes, and authorization decisions (to check whether the subject/OID is allowed to submit the claim supporting documents).

Figure 2: Asynchronous Acknowledgments with Multiple Hyper Text Transfer Protocol (HTTP) Connections



1. The HIH sends a XDR Document Submission Request to the esMD
 - The esMD system responds with a HTTP 200, as First Acknowledgement.
2. The esMD system validates the metadata and sends a First Notification to the HIH denoting success or failure validation status. The esMD system also sends the package to RC.
 - The HIH responds with a HTTP 200 in case of a successful receipt of this first notification.
 - The HIH responds with a HTTP 500 in case of a service unavailable error or internal server error.
3. Upon successful receipt of the package, the RC sends a pickup notification that is forwarded to the HIH.
 - The HIH responds with a HTTP 200 in case of a successful receipt of this pickup notification.
4. If there is an error in the receipt of the package, the RC sends a pickup failure notification that is forwarded to the HIH.
 - The HIH responds with a HTTP 200 in case of a successful receipt of this pickup failure notification.

5. For PA Programs, the RC will respond with Review Results Response which is then sent to the HIH.
 - The HIH responds with a HTTP 200 in case of a successful receipt of this Response. The HIH responds with a HTTP 500 in case of a service unavailable error or internal server error.

Note: The RC can also submit an Administrative Error response to the HIH for XDR and X12 requests. The HIH will respond with an HTTP 200 in case of a successful receipt of the Administrative Response.

5.3.2 Triggers

All requests issued by the HIH must implement the Messaging Platform Service Interface Specification and the Authorization Framework Service Interface Specification.

5.3.3 Transaction Standard

The authorization framework is based on the implementation of the OASIS WS-I Security Profile SAML Token Profile, as specified in the Messaging Platform Service Interface Specification. SAML 2.0 is the base specification for expressing assertions in the eHealth Exchange.

5.3.4 Technical Pre-Conditions

The HIH must conform to the interoperability standards:

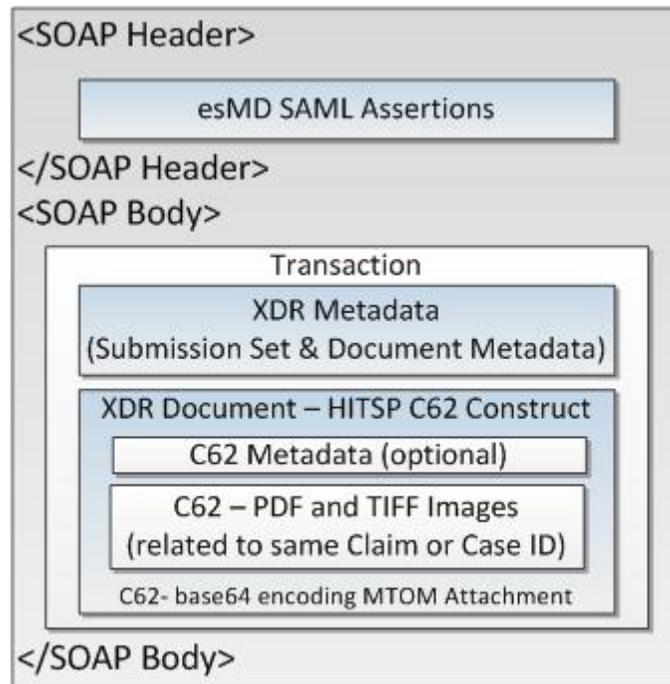
- The esMD Profile
- IHE XDR
- WS-I Basic Profile
- WS-I Basic Security Profile
- The HIH must conform to the Claim Medical Document to the Health Information Technology Standards Panel (HITSP) C62 Interoperability Specification.
- The HIHs must conform to messaging platform and authorization framework for communication.
- Messages: SOAP v2.0 with Message Transmission Optimization Mechanism (MTOM) attachments
- Service Descriptions: WSDL
- Addressing/Routing: WS-Addressing
- Security: WS-Security, XML DSIG
- Authorization: SAML Assertion
- Authentication: X509 certificate, 2-way TLS with FIPS 140-2 enable mode, 128-bit encryption.
- Base64 encoding of the C62 payload
- The esMD Document Submission data is transmitted in the SOAP message with IHE XDR transactions.
- There will be mutual authentication between the HIH Gateway and the CMS CONNECT Gateway using a Non-ONC TLS certificate.
- The CMS CONNECT Gateway will authorize the requests based on the SAML Assertions with its Home Community ID and Organization IDs.
- The HIH will create digitally signed SAML Assertions.

- A globally unique identifier, assigned by HIH internal system and primarily intended for use as a unique identifier for each submission that can be used to correlate the request and responses of a particular submission, is generated. **Note:** The Gateway created message ID is different from this unique ID.
- The HIH will encode the attached C62 document in Base64 encoding and add its hash key to the XDR metadata.
- Architectures of the HIH are decoupled from, and are opaque to, the esMD and other HIHs. The HIH need not use the same the esMD security mechanisms or standards internally.
- We suggest the initiating HIH authenticate and authorize the gateway system by sending the document submission request to the esMD project, and it is required that they do so internally. The esMD is not responsible for this action.

5.3.5 SOAP Message Envelope

Figure 3: SOAP Envelope with XDR Interchange/HITSP C62 Construct illustrates the SOAP envelope with XDR interchange and HITSP C62 construct.

Figure 3: SOAP Envelope with XDR Interchange/HITSP C62 Construct



<soapenv:Envelope

`xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"`

`xmlns:urn="urn:gov:hhs:fa:nhinc:common:nhinccomponentity"`

`xmlns:urn1="urn:gov:hhs:fa:nhinc:common:nhinccommon"`

`xmlns:add="http://schemas.xmlsoap.org/ws/2004/08/addressing"`

`xmlns:urn2="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"`

`xmlns:urn3="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"`

```

xmlns:urn4="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:urn5="urn:ihe:iti:xds-b:2007">
<soapenv:Header/>
<soapenv:Body>
  <urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>
    <urn:assertion>
      <urn:nhinTargetCommunities>
        <urn:ProvideAndRegisterDocumentSetRequest>
          </urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>
        </urn:ProvideAndRegisterDocumentSetRequest>
      </urn:nhinTargetCommunities>
    </urn:assertion>
  </urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>
</soapenv:Body>
</soapenv:Envelope>

```

The MTOM-related tags are abstracted in above soap envelope.

Table 2: Name Spaces Details with CONNECT Software lists the name space details associated with the CONNECT Software.

Table 2: Name Spaces Details with CONNECT Software

No.	Name Space	Name Space URL
1.	soapenv	http://schemas.xmlsoap.org/soap/envelope/
2.	urn	urn:gov:hhs:fha:nhinc:common:nhinccomponentity"
3.	urn1	urn:gov:hhs:fha:nhinc:common:nhinccommon
4.	add	urn:http://schemas.xmlsoap.org/ws/2004/08/addressing
5.	urn2	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
6.	urn3	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
7.	urn4	urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0
8.	urn5	urn:ihe:iti:xds-b:2007

5.3.6 SAML Assertions

The SAML Assertions define the exchange of metadata used to characterize the initiator of an HIH request so that it may be evaluated by the esMD CONNECT Gateway in local authorization decisions. The purpose of this SAML Assertion exchange is to provide the esMD CONNECT Gateway with the information needed to make an authorization decision, using the policy enforcement point for the requested esMD function. Each initiating SOAP message must convey information regarding the HIH attributes and authentication using SAML 2.0 Assertions.

5.3.7 Assertions Design Principals and Assumptions

The esMD CONNECT Gateway uses the information conveyed via the Assertions (Authorization Framework) to inform its local authorization policy decision.

The initiating HIH must include all REQUIRED attributes in each request message. It is at the discretion of the receiving esMD CONNECT Gateway to decide which attributes to consider in its local authorization decision against its policy decision controller.

The initiating HIH is responsible for the authentication and authorization of its users and system requests.

5.3.8 Assertions Transaction Standard

1. Authorization Framework v 2.0;
2. OASIS SAML V2.0;
3. Authentication Context for SAML V2.0; and
4. Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML for Healthcare Version 1.0 OASIS Web Services Security: SAML Token Profile 1.1 specifications.

5.3.9 Specific Assertions

The SAML Assertions in Table 3: Standard SAML Assertions in SOAP Envelope are designated, as required (R), for all communications between the HIH and the esMD CONNECT Gateway.

Table 3: Standard SAML Assertions in SOAP Envelope

Parent Element	Child Element / Attribute	esMD Required	Who Create? - Gateway or Manual
SAML ASSERTION (Required)	Version	Required	CONNECT Gateway
SAML ASSERTION (Required)	ID	Required	CONNECT Gateway
SAML ASSERTION (Required)	IssueInstant	Required	CONNECT Gateway
SAML ASSERTION (Required)	Issuer	Required	CONNECT Gateway
SAML ASSERTION (Required)	Subject	Required	CONNECT Gateway
Authn Statement (Required)	AuthnContext	Required	HIH Application will add under assertion
Authn Statement (Required)	SubjectLocality	Required	HIH Application will add under assertion
Authn Statement (Required)	AuthnInstant	Required	HIH Application will add under assertion
Authn Statement (Required)	SessionIndex	Optional	HIH Application will add under assertion
Attribute Statement (Required)	subject-ID	Required	CONNECT Gateway
Attribute Statement (Required)	organization	Required	HIH Application will add under assertion

Parent Element	Child Element / Attribute	esMD Required	Who Create? - Gateway or Manual
Attribute Statement (Required)	homeCommunityID	Required	HIH Application will add under assertion
Attribute Statement (Required)	purposeofuse	Required	HIH Application will add under assertion
Attribute Statement (Required)	NPI	Required	HIH Application will add under assertion – ‘userInfo.userName’ or as nationalProviderId (for CONNECT, Version 4.0 and greater).
Attribute Statement (Required)	Intended Recipient	Required	HIH Application will add under assertion - ‘uniquePatientId’.
Authorization Decision Statement (Optional)	Action	Required	HIH Application will add under assertion, if Authorization Decision Statement is provided.
Authorization Decision Statement (Optional)	Decision	Required	HIH Application will add under assertion, if Authorization Decision Statement is provided.
Authorization Decision Statement (Optional)	Resource	Required	HIH Application will add under assertion, if Authorization Decision Statement is provided.
Authorization Decision Statement (Optional)	Evidence	Required	HIH Application will add under assertion, if Authorization Decision Statement is provided.

5.3.10 The esMD SAML Assertion Details

Table 4: The esMD SAML Assertion Details provides the esMD SAML Assertion details.

Table 4: The esMD SAML Assertion Details

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
1.	homeCommunityId	<p><urn1:homeCommunityId ></p> <p> <urn1:description>Description of the submitting HIH CONNECT or CONNECT Compatible Gateway</urn1:description></p> <p><urn1:homeCommunityId>urn:oid:1.3.6.1.4.1.101420.6.1</urn1:homeCommunityId></p> <p> <urn1:name>Name of the submitting HIH CONNECT or CONNECT Compatible Gateway</urn1:name></p> <p></urn1:homeCommunityId></p>	R	The esMD Requirement / Yes	HIH OID
2.	organizationId	<p><urn1:organizationId ></p> <p> <urn1:description>Description of Broker Organization between provider and the submitting HIH CONNECT or CONNECT Compatible Gateway</urn1:description></p> <p><urn1:homeCommunityId>urn:oid:1.3.6.1.4.1.101420.6.1</urn1:homeCommunityId></p> <p> <urn1:name>Name of Broker Organization between provider and the submitting HIH CONNECT or CONNECT Compatible Gateway</urn1:name></p> <p></urn1:organizationId></p>	R	esMD Requirement / Yes	HIH OID or any broker organization (it's OID) between providers and HIH

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
3.	intendedRecipient	<p>Note: Temporarily, add the Intended Recipient value in the unique Patient ID as OID.</p> <p><urn1:uniquePatientId>urn:oid:2.16.840.1.113883.13.34.110.1.110.9</urn1:uniquePatientId></p> <p>In the next spec factory changes, the intended recipient values will be change to HL7 XON.</p> <p>The intendedRecipient field in the XDS Metadata will use the HL7 XON data type for this profile.</p> <p>This data type contains 10 subfields separated by a ^ sign, of which three are required:</p> <p>XON.1 is the name of the organization that is the intended recipient. This will be the name of the RA that is intended to receive the submission.</p> <p>XON.6 identifies the assigning authority for the identifiers appearing in XON.10. This field will be completed using the following string: <i>&CMS OID FOR RAS&ISO</i> [ed. Note: Replace CMD OID FOR RAS with a CMS assigned OID].</p> <p>XON.10 is the CMS Identifier for the RA. An example appears below (bold text should be replaced with the appropriate values): [Ed. Note: Replace CMD OID FOR RAs with a CMS assigned OID].</p> <p>RA ORGANIZATION NAME^^^^^&CMS OID FOR RAS&ISO^^^^^CMS ASSIGNED IDENTIFIER<urn1:intendedReceipient ></p>	R	esMD Requirement / NO*	Refer to section 5.3.23 Intended Recipients Attribute

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
3. Cont.	No additional information	<p><urn1:description>Description of receiving Review Contractor</urn1:description></p> <p><urn1:organizationId>DCS^^^^&2.16.840.1.113883.13.34.110.1.100.1&ISO^^^^2.16.840.1.113883.13.34.110.1</urn1:organizationId></p> <p><urn1:name>Name of Review Contractor, to whom Claim Medical Documentation shall be submitted.</urn1:name></p> <p></urn1:intendedRecipient></p>	No additional information	No additional information	No additional information

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
4.	NPI	<p>In Release 4.0, the NPI value can be sent in a new element NationalProviderId added to the assertion element of the RespondingGateway_ProvideAndRegisterDocumentSetRequest.</p> <p>The esMD system will continue to support the Release 3.1 format for sending the NPI, as the value for the userInfo/username for the RespondingGateway_ProvideAndRegisterDocumentSetRequest</p> <pre> <urn1:userInfo> <urn1:userName>6101234512</urn1:userName> <urn1:org> <urn1:description>Description of provider NPI </urn1:description> <urn1:homeCommunityId>Any Broker organization in between provider and HIH or HIH OID</urn1:homeCommunityId> <urn1:name>Name of provider from whom Claim Medical Documentation are submitted</urn1:name> </urn1:org> </urn1:userInfo> </pre> <p>Note: The National provider Identifier (NPI) value needs to be 10 numeric characters long to comply with the standard specification. If the NPI value sent by the HIH does not conform to this format, the submission request shall be rejected and an error message will be sent to the submitting HIH gateway. Please refer to Table 19: Sample Error Message Content for the error code and related message text.</p>	R	esMD Requirement / NO*	Refer to section 5.3.22 National Provider Identifier (NPI) Attribute

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
5.	purposeOfDisclosureCoded	<p>HIH will enter appropriate values. This is used by the CONNECT Gateway for SOAP header SAML processing.</p> <pre> <urn1:purposeOfDisclosureCoded> <urn1:code>PAYMENT</urn1:code> <urn1:codeSystem>2.16.840.1.113883.3.18.7.1</urn1:codeSystem> <urn1:codeSystemName> esMD CMS Purpose</urn1:codeSystemName> <urn1:codeSystemVersion>1.0</urn1:codeSystemVersion> <urn1:displayName>Medical Claim Documentation Review</urn1:displayName> <urn1:originalText>Medical Claim Documentation Review</urn1:originalText> </urn1:purposeOfDisclosureCoded> </pre>	R	esMD Requirement / Yes	

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
6.	samlAuthnStatement	<p>HIH will enter appropriate values. This is used by the CONNECT Gateway for SOAP header SAML processing.</p> <pre> <urn1:samlAuthnStatement> <urn1:authInstant>2011-01-05T16:50:01.011Z</urn1:authInstant> <urn1:sessionIndex>987</urn1:sessionIndex> <urn1:authContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509< /urn1:authContextClassRef> <urn1:subjectLocalityAddress>158.147.185.168</urn1:subjectLocalityAddr ess> <urn1:subjectLocalityDNSName>cms.hhs.gov</urn1:subjectLocalityDNSNa me> </urn1:samlAuthnStatement> </pre>	R	esMD Requirement / Yes	

7.	samlAuthzDecisionStatement	<p>Except ID attribute in samlAuthzDecisionStatement, all the other appropriate values will be entered by HIH.</p> <p>ID attribute will be used by the esMD application and other values will be used by the CONNECT Gateway for SOAP header SAML processing.</p> <p>ID attribute will be used to correlate the request to response and to verify the double submission of Claim Document submission. Each Claim Document Submission SOAP Message from CONNECT Gateway will have a Unique ID populated by HIH CONNECT Adapter or CONNECT Compatible software.</p> <p>This unique ID will be created by HIH using the JAVA UUID API and populate into "id" attribute of this SAML Authorization Decision Statement.</p> <p><urn1:id>40df7c0a-ff3e-4b26-baeb-f2910f6d05a9</urn1:id></p> <p>Note: Unique ID is different from CONNECT Gateway Message ID. CONNECT Gateway automatically adds the message id to the SOAP Header. This message ID is unique for any outgoing messages.</p> <p><urn1:samlAuthzDecisionStatement ></p> <p> <urn1:decision>Permit</urn1:decision></p> <p><urn1:resource>https://158.147.185.168:8181/esMD/DocumentSubmission</urn1:resource></p> <p>;2 <urn1:action>TestSaml</urn1:action></p> <p> <urn1:evidence></p> <p> <urn1:assertion></p>	R	esMD Requirement / Yes	
7. Cont.	No additional information	<p><urn1:id>40df7c0a-ff3e-4b26-baeb-f2910f6d05a9</urn1:id></p> <p><urn1:issueInstant>2011-01-05T16:50:01.011Z</urn1:issueInstant></p>	No additional information	No additional information	No additional information

No.	SAML Assertion Attribute	Definition and Example	Required (R)/ Required if known (R2)/ Optional (O)	Source / CONNECT Software Allowed	References to the esMD Domain Specific Values
		<pre> <urn1:version>2.0</urn1:version> <urn1:issuerFormat>urn:oasis:names:tc:SAML:1.1:nameid- format:X509SubjectName</urn1:issuerFormat> <urn1:issuer>CN=HIH SAML User,OU=QSSI,O=QSSI,L=Baltimore,ST=MD,C=US</urn1:issuer> <urn1:conditions> <urn1:notBefore>2011-01-05T16:50:01.011Z</urn1:notBefore> <urn1:notOnOrAfter>2011-01- 05T16:53:01.011Z</urn1:notOnOrAfter> </urn1:conditions> ; <urn1:accessConsentPolicy>Claim-Ref-1234 NA for the esMD</urn1:accessConsentPolicy> <urn1:instanceAccessConsentPolicy>Claim-Instance-1 NA for the esMD</urn1:instanceAccessConsentPolicy> </urn1:assertion> </urn1:evidence> </urn1:samlAuthzDecisionStatement> </pre>			

* The Interim solution is to populate the 'Intended Recipient' and 'NPI' values into 'uniquePatientId' and 'userInfo.userName' field of the current CONNECT software Assertion Type object.

5.3.11 SAML Assertion Attributes

This will be added in the Authorization Decision Statement.

5.3.12 Version Attribute

The version attribute defines SAML v2.0, as the version.

5.3.13 ID Attribute

The ID Attribute is an xs:ID, as defined by <http://www.w3.org/TR/xml-Id/>.

5.3.14 Issue Instant

The Issue Instant attribute is an xs:dateTime, as defined by <http://www.w3.org/TR/xmlschema-2/>.

5.3.15 Issuer

The <Issuer> element identifies the individual gateway system responsible for issuing the Assertions carried in the message. Since the esMD does not have the user's IDs, the issuer will be the HIH's System Name. This element includes a NameID format attribute, which declares the format used to express the value contained in this element. The NameID format is ***urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName*** for sending NHIO, acting as a node on the eHealth Exchange.

5.3.16 Subject

The Subject element will identify the Subject of the assertion. This element also includes a NameID. The Format attribute declares the format used to express the value contained in this element: the HIH's System Name making the request at the initiating NHIO. The NameID format is ***urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName*** for the sending the NHIO.

5.3.17 SAML Statement Elements

The esMD SAML statement elements are separated into Authentication and Attribute. Each statement will be further defined in the following paragraphs.

5.3.18 Attribute Statement

The Attribute Statement element describes a statement by the SAML authority asserting that the requesting HIH system is associated with the specified attributes. The Attribute Statement is required to contain attribute elements, as defined by the OASIS XSPA profile of SAML and described in the sections that follow. The Attribute Statement is comprised of the following attributes: Subject ID, Subject Organization, Home Community ID, Purpose of Use, NPI, and Intended Recipient.

The value on the Subject ID and Subject Organization attributes will be a plain text description of the user's name (not user ID) and organization, respectively. These are primarily intended to support auditing.

5.3.19 Subject ID Attribute

This Subject Identifier element has the HIH initiating gateway Name. The name of the system, as required by HIPAA Privacy Disclosure Accounting is placed in the value of the element.

```
<urn1:QualifiedSubjectIdentifier xmlns:urn1="urn:gov:hhs:fha:nhinc:common:nhinccommon">  
  <urn1:SubjectIdentifier>HIH esMD Initiating Gateway </urn1:SubjectIdentifier >  
  <urn1:AssigningAuthorityIdentifier>HIH Name</urn1: AssigningAuthorityIdentifier >
```

</ urn1:QualifiedSubjectIdentifier>

Subject Organization Attribute

This Assigning Authority Identifier element has the subject organization Name under which the initiating gateway (subject name) is running. In plain text, the organization to which the user belongs, as required by HIPAA Privacy Disclosure Accounting, is placed in the value of the Attribute Value element.

```
<urn1:QualifiedSubjectIdentifier xmlns:urn1="urn:gov:hhs:fha:nhinc:common:nhinccommon">
  <urn1:SubjectIdentifier>HIH esMD Initiating Gateway </urn1: SubjectIdentifier >
  <urn1:AssigningAuthorityIdentifier>HIH Name</urn1: AssigningAuthorityIdentifier >
</ urn1:QualifiedSubjectIdentifier>
```

5.3.20 Home Community ID Attribute

This attribute element has the HIH gateway Name attribute. The value is the HL7 issued Home Community ID (an Object Identifier) assigned to the HIH that is initiating the request, using the URN format (i.e., "urn:oid:" appended with the OID). One home community gateway can have multiple organization IDs. Organization IDs act as a broker to home community organizations. If there are no brokers to the organizations, then both the home community ID and the organization ID attributes will be the same.

Refer to the sample in Table 4: The esMD SAML Assertion Details.

5.3.21 Purpose of Use Attribute

This attribute element has the purpose of use disclosure Name attribute. The value of the attribute element is a child element, "PurposeOfUse", in the namespace "urn:hl7-org:v3", whose content is defined by the "CE" (coded element) data type from the HL7 version 3 specification. The PurposeOfUse element contains the coded representation of the Purpose for Use that is, in effect, for the request. The PurposeOfUse is defined in Authorization Framework document. Refer to the sample in Table 4: The esMD SAML Assertion Details.

5.3.22 National Provider Identifier (NPI) Attribute

An NPI is a unique ten (10)-digit identification number issued to health care providers in the United States by the CMS. This attribute provides the ability to specify an NPI value, as part of the SAML Assertion that accompanies a message that is transmitted across the eHealth Exchange.

In Release 4.0, the NPI value can be sent in a new element **NationalProviderId** that has been added to the **assertion** element of the RespondingGateway_ProvideAndRegisterDocumentSetRequest.

The esMD system will continue to support the existing format for sending the NPI, as the value for the **userInfo/username** for the RespondingGateway_ProvideAndRegisterDocumentSetRequest.

5.3.23 Intended Recipients Attribute

Intended Recipients are RCs, to whom the esMD needs to send the HIH submitted Claim Medical documentation payloads. The valid values are addressed in Table 5: The esMD Functional Specific Submission Set Metadata Attributes.

5.3.24 Authentication Statement

The SAML Authentication Assertions are associated with authentication of the Subject (HIH Gateway Identification). The <AuthnStatement> element is required to contain an <AuthnContext> element and an AuthnInstant attribute. The SAML AuthnStatement contains one AuthnContextClassRef element identifying the method by which the subject was authenticated. Other elements of SAML AuthnStatement include <SubjectLocality> element and a SessionIndex attribute. The saml:Authentication is comprised of the four Attributes or Elements: AuthnContext, Subject Locality, AuthnInstant, and Session Index.

5.3.25 Authentication Method (AuthnContext)

An authentication method, the <AuthnContext> element indicates how that authentication was done. **Note:** The authentication statement does not provide the means to perform that authentication, such as a password, key, or certificate. This element will contain an authentication context class reference.

Authentication Method - X.509 Public Key

URN - urn:oasis:names:tc:SAML:2.0:ac:classes:X509

5.3.26 Subject Locality

Subject Locality references from where the user was authenticated. The Subject Locality element specifies the Domain Name System (DNS) domain name and IP address for the system entity that was authenticated.

5.3.27 Authentication Instant (AuthnInstant)

The Authentication Instant, <AuthnInstant>, attribute specifies the time at which the authentication took place which is an xs:dateTime, as defined by <http://www.w3.org/TR/xmlschema-2/>.

5.3.28 Session Index

The Session Index, *SessionIndex*, attribute identifies the session between the Subject and the Authentication Authority.

5.3.29 Example

Refer to the sample in Table 4: The esMD SAML Assertion Details.

5.3.30 Authorization Decision Statement

This is an optional element that could convey all valid NPI submissions.

The *Authorization Decision Statement* element describes a statement by the SAML authority asserting that a request for access, by the statements subject to the specified resource, has resulted in the specified authorization decision based on some optionally specified evidence. This element provides the HIH an opportunity to assert that it holds an Access Consent Policy which the esMD CONNECT Gateway may wish to evaluate in order to determine if access to the requested resource(s) should be allowed for the submitted provider.

The information conveyed within the Authorization Decision Statement may be used by the esMD CONNECT Gateway to retrieve the asserted Access Consent Policy. The format of the Access Consent Policy is defined in the Access Consent Policy specification.

The Authorization Decision Statement will be used when the provider has granted permission to submit the documentation to the esMD CONNECT Gateway, and the HIH needs to make that authorization known to the esMD CONNECT Gateway.

The Authorization Decision Statement has the following content: Action, Decision, Resource, Evidence, and Assertions.

5.3.31 Action

This action must be specified using a value of Execute.

5.3.32 Decision

The Decision attribute of the Authorization Decision Statement must be Permit.

5.3.33 Resource

The Resource attribute of the Authorization Decision Statement must be the Uniform Resource Identifier (URI) of the endpoint to which the esMD CONNECT Gateway request is addressed or an empty URI reference.

5.3.34 Evidence

The Authorization Decision Statement must contain an <Evidence> element, containing a single <Assertion> child element.

5.3.35 Assertions

This <Assertion> element must contain an ID attribute, an IssueInstant attribute, a Version attribute, an Issuer element, and an Attribute Statement element. Refer to Section 5.3.7, The esMD Functional Specific Submission Set Metadata Attributes for more details on building the Assertion.

There must be at least one of the following Attributes in the Attribute Statement.

- An <Attribute> element with the name AccessConsentPolicy and NameFormat. The value(s) for this attribute will be the OIDs of the access policies that the asserting entity has previously agreed to with other entities. The OIDs MUST be expressed, using the urn format (e.g., - urn:oid:1.2.3.4). See the following example:

```
<saml2:Attribute Name="AccessConsentPolicy"  
NameFormat="http://www.hhs.gov/healthit/nhin">  
  <saml2:AttributeValue>urn:oid:1.2.3.4</saml2:AttributeValue>  
</saml2:Attribute>
```

- An <Attribute> element with the name InstanceAccessConsentPolicy and NameFormat, for example, <http://www.hhs.gov/healthit/nhin>. The value(s) of this attribute will be the OIDs of the patient specific access policy instances. The OIDs MUST be expressed, using the urn format (e.g., - urn:oid:1.2.3.4.123456789). If a requestor specifies this Attribute, the requestor MUST support the ability for the specified policy document(s) to be retrieved via the transactions defined in HITSP TP30. See the following example:

```
<saml2:Attribute Name="InstanceAccessConsentPolicy"  
NameFormat="http://www.hhs.gov/healthit/nhin">  
  <saml2:AttributeValue  
xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance"
```

```

xmlns:ns7="http://www.w3.org/2001/XMLSchema"
ns6:type="ns7:string">urn:oid:1.2.3.4.123456789
</saml2:AttributeValue>
</saml2:Attribute>

```

- The "ContentReference", "ContentType", and "Content" attributes from the Trial Implementation specifications have been removed and should no longer be used. Refer to the sample in Table 4: The esMD SAML Assertion Details.

Note: For more details, please refer to: <http://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v3.0.pdf> and go to Section 3.2.3.

5.3.36 Target Communities

The target communities must specify the targeted the esMD CONNECT Gateway OID details. It contains three values:

- **Description:** The esMD CONNECT Gateway with an XDR document submission endpoint to accept claim related document submissions to the esMD ;
- **HomeCommunityId:** The esMD CONNECT Gateway Home Community ID (OID); and
- **Name:** The Name of the esMD CONNECT Gateway Home Community ID (OID).

```

<urn:nhinTargetCommunities>
  <urn1:homeCommunity>
    <urn1:description>
      esMD CONNECT Gateway Home Community ID Description
    </urn1:description>
    <urn1:homeCommunityId>urn:oid:1.3.6.1.4.1.101420.6.1</urn1:homeCommunityId>
    <urn1:name>Name of the esMD CONNECT Gateway Home Community
  ID<urn1:name>
  </urn1:homeCommunity>
</urn:nhinTargetCommunities>

```

For CMS response Message to HIH, these nhinTargetCommunities will have the HIH OID information.

5.3.37 Metadata Fields

The HIH adopts the IHE Cross Enterprise Document Reliable Interchange (XDR) profile in a SOAP envelope with an XDS Repository Submission Request-Provide and Register Document set, b (ITI-41) transaction metadata and C62 document payload with MTOM, Base64 encoded attachments.

```

<urn:ProvideAndRegisterDocumentSetRequest>
<urn2:SubmitObjectsRequest id="999" comment="comment">

```

```

    <urn4:RegistryObjectList>
    <urn4:ExtrinsicObject id="Document01" mimeType="application/pdf"
    objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
        <urn4:RegistryPackage id="SubmissionSet01">
            <urn4:Classification id="classification01" classifiedObject="SubmissionSet01"
            classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"/>
            <urn4:Association id="association01" associationType="HasMember"
            sourceObject="SubmissionSet01" targetObject="Document01">
        </urn4:RegistryObjectList>
    <urn2:SubmitObjectsRequest>
    <urn5:Document id="Document02">
        <ClinicalDocument ... (Encoded Message)
        .....
        <nonXMLBody>
        2PD943454OIJKD2lvbj0iMS4wliBlbmNvZGluZz0iVVRGLTgiPz4NjxDbGluaWNhbERvY3VtZW5=
        </nonXMLBody>
    </ClinicalDocument>
    </urn5:Document>
    <urn5:Document id="Documentnn">
    nnPD94bWwgdIvbj0iMS4wliBlbmNvZGluZz0DLKFALDFALDECjxDbGluaWNhbERvY3VtZW5=
    </urn5:Document>
    </urn:ProvideAndRegisterDocumentSetRequest>
  
```

A “SubmitObjectsRequest” is a collection of repository metadata of multiple MTOM base64 encoded document attachments transferred between an HIH and the esMD Gateway.

An ExtrinsicObject (XSDDocumentEntry) represents a single attached document metadata in the XDR the esMD Document Submission SOAP message, which refers to its attached document.

A “RegistryPackage” is a collection of repository metadata of just one MTOM base64 encoded document.

Following are the esMD Functional (mandatory) and Transmission (mandatory) metadata elements needed for the esMD Gateway to process the submitted claim medical document. For further details on each of the tags, review XDS IHE_ITI_TF Volume 3, Revision 6.

5.3.38 The esMD Functional Specific Submission Set Metadata Attributes

Table 5: The esMD Functional Specific Submission Set Metadata Attributes details the esMD Functional Specific Submission Set Metadata Attributes to confirm with the IHE ITI Technical Framework Volume 3, Revision 6, and XDR Interoperability Testing.

The following table indicates if the esMD XDR Submission Set metadata attributes are required (R), required if known (R2), optional (O) and XML Element Not Required (NR). To confirm the IHE XDR interoperability test, add xml tag with the value as “NA”, if R2 or Optional.

Note: As of Release 3.1, a Claim ID for First level Appeal Requests is optional.

Table 5: The esMD Functional Specific Submission Set Metadata Attributes

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
1.	esMDClaimId	<p>Claim Identifier is the identifier with which the provider submits the Claim to the esMD. It can be found in the Additional Documentation Request (ADR) letter from the RC and needs to be used to submit:</p> <ul style="list-style-type: none"> Documents in response to ADR from the CMS RC(s); and RA Discussion Requests. <p>Note 1: The esMD "ClaimId" value for documents sent in responses to an ADR and RA Discussion Requests submissions need to be in one of the following formats or the submission shall be rejected:</p> <ul style="list-style-type: none"> 13 numeric characters in length; or 14 numeric characters in length; or 15 numeric characters in length; or 17 – 23 variables characters in length (can include alphabets, numbers, dashes and spaces). <p>From the esMD Release 3.0 onwards, HIH/providers shall submit the ADR and RA Discussion Requests, with the esMDClaimId in either of the following two formats (to enable backward compatibility):</p>	R Note: While the Claim ID for the First Level Appeal Requests and Second Level Appeal Requests are optional, HIHs are encouraged to include it.	NR	NR Note: If a Claim Id is sent for an ADCM request, the Claim Id will be ignored and will not be sent to the RC.	esMD Requirement	ADR Letter	HL7 CX data type with string (76)

1. Cont 1	No additional information	<p>Note: Claim ID length greater than 256 for First Level and Second Level Appeal requests will be rejected by the esMD system. The format of the Composite Claim ID is validated for both First Level Appeal requests and Second Level Appeal requests.</p> <p>The esMD Claim Id could be sent in two of the following formats; however, it is recommended for the HIH to submit the Claim Id in the Standard Format.</p> <p>a. the HL7 CX composite format, which contains two components, the Claim Id number, and the Assigning Authority (AA) like the CMS RC, which identifies the domain over which the Claim ID number represents a unique entity. The composite format looks like so: <i>Claim ID^^^&RC OID&ISO</i></p> <p>Note 2: The ampersand “&” character must be properly encoded, for example “&amp”, in the XML content.</p> <p>Note 3: For submissions sent with the name “esMDClaimID”(i.e., with an upper Claim ID) for the ClaimId slot, the submission will be rejected and they will not be passed on to the RC.</p> <p>Note4: In the example below the Claim Id value is 13 numeric characters:</p> <pre><urn4:Slot name="esMDClaimId"> <urn4:ValueList> <urn4:Value>1234567890123^^^&amp;2.16.840.1.113883.13.34.110.1.100.1&amp;ISO</urn4:Value></pre>	No additional information					
1. Cont 2	No additional information	<pre></urn4:ValueList> </urn4:Slot></pre> <p>Note5: If there are any errors in the composite format, or in the format/length of the esMD Claim Id, the_submission shall be rejected.</p> <p>b. Or HIHs can send just the esMD Claim Id alone, as displayed in the example below:</p>	No additional information					

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
		<p><urn4:Slot name="esMDClaimId"> <urn4:ValueList> <urn4:Value>1234567890123</urn4:Value> </urn4:ValueList> </urn4:Slot></p> <p>Note6: If there are any errors in the format/length of the Claim ID, the submission shall be rejected.</p> <p>Power Mobility Device (PMD) Prior Authorization (PA) Requests, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests: DMEPOS PA request, and HHPCR demonstration requests Documentation submissions sent in reference to the aforementioned lines of business shall NOT have the esMD Claim Id. HIHs are advised to send submissions relating to PMD PA Requests, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests, DMEPOS PA request, and HHPCR demonstration requests without the XML tag for the esMD Claim Id field. If HIHs send a value for the esMDClaimId attribute, the submission shall be rejected.</p>						

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
2.	esMDCaseld	<p>Case Identifier is the identifier, generated by the RC to open a claim specific case. This could be found in Additional Documentation Request (ADR) letter from the RC if the request is from MACs. It can be used to submit:</p> <ul style="list-style-type: none"> Documents in response to Additional Documentation Request (ADR) RA Discussion Requests and <p>For submissions to the PERM RC, HIHs/providers need to send the 11 alphanumeric characters PERM ID they get on the ADR from PERM, in the esMDCaseld tag.</p> <p>From the esMD Release 3.0., for submissions related to responses to an ADR and RA Discussion Requests, HIHs/providers shall have a choice to send the esMDCaseld in either of the following two formats (to enable backward compatibility):</p> <ol style="list-style-type: none"> The esMDCaseld could be sent in the HL7 CX composite format, which contains two components: the Case Id number and the Assigning Authority (AA) (i.e., the CMS RC that identifies the domain over which the Case Id number represents a unique entity). The composite format: <i>Case Id^^^&RC OID&ISO</i> 	R2	R	NR	esMD Requirement	ADR Letter (if MAC is the RC)	HL7 CX data type with string (76)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
2. Cont. 1	No additional information	<p>Note 1: The '&' character must be properly (like &amp;) encoded in the XML content:</p> <pre> <urn4:Slot name="esMDCaseld"> <urn4:ValueList> <urn4:Value>12345678901234567890AB^^^&amp;2.16.84 0.1.113883.13.34.110.1.100.1&amp;ISO </urn4:Value> </urn4:ValueList> </urn4:Slot> </pre> <p>Note 2: Submissions (other than ADR PERM), sent with the name as "esMDCaseld"(i.e., with an uppercase ID) for the Caseld slot, will receive a blank Case ID value in the RC metadata XML file. For an ADR PERM request, sent with the name as "esMDCaseld"(i.e., with an uppercase ID) for the Caseld slot, the submission will be rejected and will not be passed on to the RC.</p> <p>b. HIHs can send just the esMDCaseld alone, as displayed in the example below:</p> <pre> <urn4:Slot name="esMDCaseld"> <urn4:ValueList> <urn4:Value>12345678901234567890AB </urn4:Value> </urn4:ValueList> </urn4:Slot> </pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
2. Cont. 2	No additional information	<p>Note 1: Documentation sent in reference to PMD PA Requests, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests, DMEPOS PA requests, and HHPCR Demonstration requests shall NOT have the esMDCaseld. HIHs are advised to send submissions relating to PMD PA Requests, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests, DMEPOS PA requests, and HHPCR Demonstration requests without the XML tag for the esMDCaseld element.</p> <p>Note 2: If HIHs pass the esMDCaseld tag or a value for this tag, the submission shall be rejected.</p>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
3.	IntendedRecipient	<p>Intended Recipient represents the organization(s) or person(s) for whom the Document Submission set is intended for:</p> <p>In the esMD, the Intended Recipient will be an organization (RC) to whom the sender (HIH) will submit the message with the esMD Claim supporting Documents. This Intended Recipient will be identified by a HL7 issued organizational identifier (OID)</p> <p>Example: RC OID</p> <pre><urn4:Slot name="intendedRecipient"> <urn4:ValueList> <urn4:Value>2.16.840.1.113883.13.34.110.2.100.1</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol. 3	Refer to Section 5.3.23 Intended Recipients Attribute	String (64)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
4.	Author	<p>Represents the provider (NPI), who submits the Claim Supporting Documents. This document submission could be in response to an Additional Documentation Request letter (ADR) from a CMS RC, First Level Appeal Requests, RA Discussion Requests, ADMC Requests, PMD PA, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests, DMEPOS PA requests, and HHPCR Demonstration requests.</p> <p>This attribute could either contain the following sub-attributes based on who (either provider or institution NPI) submits the documentation:</p> <p>This is the esMD Required Field.</p>	R	R	R	IHE ITI TF Rel. 6 Vol.3	<p>NPI</p> <p>Table 4.1-5 Document Metadata Attribute Definition in IHE ITI TF Volume 3 Revision 6.0 (http://www.ihe.net/Technical_Framework/up_load/IHE_ITI_TF_6-0_Vol3_FT_2009-08-10-2.pdf)</p>	Numeric (10)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
4. Cont	No additional information	authorInstitution authorPerson <pre> <urn4:Classification id="cl08" classificationScheme="urn:uuid: a7058bb9-b4e4-4307- ba5b-e3f0ab85e12d" classifiedObject=" SubmissionSet01" nodeRepresentation="author"> <urn4:Slot name="authorInstitution"> <urn4:ValueList> <urn4:Value>604123</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Slot name="authorPerson"> <urn4:ValueList> <urn4:Value>603111</urn4:Value> </urn4:ValueList> </urn4:Slot> </urn4:Classification> </pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
5.	authorInstitution (sub-attribute of author)	<p>If there is only one document in the SubmissionSet, authorInstitution attribute of the SubmissionSet will have the same NPI as the one used in the authorInstitution attribute at the document level.</p> <p>If there is more than one document in the SubmissionSet, authorInstitution attribute of the SubmissionSet will have the NPI of the organization/institution, which put together all the documents, included in the SubmissionSet.</p> <p>Note: At the SubmissionSet level, either the authorInstitution or the authorPerson attribute will be used but never both.</p> <pre data-bbox="401 954 779 1157"><urn4:Slot name="authorInstitution"> <urn4:ValueList> <urn4:Value>604123</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R2	R2	R2	IHE ITI TF Rel. 6 Vol.3	NPI Institution Name	Numeric (10)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
5.1.	authorPerson (sub-attribute of author)	<p>If there is only one document in the SubmissionSet, authorPerson attribute of the SubmissionSet will have the same NPI as the one used in the authorPerson attribute at the document level.</p> <p>If there is more than one document in the SubmissionSet, authorPerson attribute of the SubmissionSet will have the NPI of the provider who put together all the documents in the SubmissionSet.</p> <p>Note: At the SubmissionSet level, either the authorInstitution or the authorPerson attribute will be used but never both.</p> <pre data-bbox="405 954 793 1157"><urn4:Slot name="authorPerson"> <urn4:ValueList> <urn4:Value>603111</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R2	R2	R2	IHE ITI TF Rel. 6 Vol.3	NPI Person or Machine Name	Numeric (10)
6.	Comments	<p>Comments associated with the Submission Set in free form text.</p> <pre data-bbox="384 1276 968 1417"><urn4:Description> <urn4:LocalizedString value="esMD Claim Document Submission in response to Review Contractor ADR Letter"/> </urn4:Description></pre>	O	O	O	IHE ITI TF Rel. 6 Vol.3		String (256)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
7.	ContentTypeCode	<p>The ContentTypeCode identifies the line of business for which the provider/HIH/ is sending the submission request. the submission request could be:</p> <ul style="list-style-type: none"> • A response to the CMS RC ADR letter • First Level Appeal Requests • Second Level Appeal Requests • RA Discussion Requests • Advance Determination of Medicare Coverage (ADMC) Requests • Power Mobility Device Prior Authorization Requests (PMD PA) • Non-Emergent Ambulance Transport PA Requests, or • Hyperbaric Oxygen PA Requests <p>The ContentTypeCode is the code that specifies to which line of business (responses to ADR, First Level Appeal Requests, Second Level Appeal Requests, RA Discussion Requests, ADCMC Requests, PMD PA, Non-Emergent Ambulance Transport PA Requests, or HBO PA Requests) the submission request belongs.</p> <p>Note1: Refer to Table 8: Content Type Codes and Corresponding Content Type Code Display Names for more details on the Content Type Codes.</p>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Refer to 5.3.41 Content Type Code	String (16)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
7. Cont	No additional information	<p>Note2: In the example below, the Content Type Code with a value of '1' is used which specifies that this submission request is in response to an Additional Documentation Request (ADR).</p> <pre> <urn4:Classification id="cl09" classificationScheme="urn:uuid:aa543740-bdda-424e-8c96- df4873be8500" classifiedObject="SubmissionSet01" nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000. 1"> <urn4:Slot name="ContentTypeCode"> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="Response to Additional Documentation Request (ADR)"/> </urn4:Name> </urn4:Classification> </pre> <p>Note2: Refer to 5.3.41 Content Type Code for additional values.</p>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
8.	entryUUID	<p>A unique ID or a globally unique identifier within the document submission request for the SubmissionSet. For example, “<i>SubmissionSet01</i>” can be <i>entryUUID</i>. It can also be in the UUID format.</p> <p>In the below example, “<i>SubmissionSet01</i>” is used as <i>entryUUID</i>. This can also be UUID format.</p> <p>Example:</p> <pre><urn4:RegistryPackage id="SubmissionSet01"> </urn4:RegistryPackage></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Unique Name for each attached document with a submitted document. Either UUID or some unique identifier.	String (64)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
9.	patientID	<p>As per XDR specification, this metadata attribute is mandatory. Currently the esMD does not handle patientID.</p> <p>For ADR, First Level Appeal Requests, Second Level Appeal Requests, and RA Discussion Requests, use case submissions. HIHs/providers need to submit the esMDClaimId value in this patientID metadata attribute as follows:</p> <p>The ClaimId value needs to be sent in the standard format or the HL7 composite format as mentioned under the esMDClaimId metadata attribute.</p> <p>Note 1: The ‘&’ character must be properly (like &amp;) encoded in the XML content.</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="1234567890123^^^&amp;2.16.840.1.113883.13.34 &amp;ISO"></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	CMS RC OID.ClaimID	HL7 CX data type with String (256)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADCMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
9. Cont 1	No additional information	<pre> <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier> Note 2: To enable backward compatibility, HIHs/providers may submit this patientID metadata attribute with the esMDClaimId value in the standard format (No HL7 composite format) as follows: <urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="1234567890123"> <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier> </pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
9. Cont 2	No additional information	<p>For PMD PA, Non-Emergent Ambulance Transport PA Requests, HBO PA Requests, DMEPOS, and HHPCR Demonstration requests use case submissions (since there is no ClaimId value), HIHs/providers may submit the value of "NA" in the HL7 composite format as follows:</p> <pre> <urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA^^^&2.16.840.1.113883.13.34&ISO" > <urn4:Name> <urn4:LocalizedString value="XDSDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier> </pre> <p>Note 3: To enable backward compatibility, HIHs/providers may submit this patientID metadata attribute with the esMDClaimId value in standard format (No HL7 composite format):</p>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
9. Cont 3	No additional information	<p><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA" ></p> <p><urn4:Name></p> <p><urn4:LocalizedString value="XSDSDocumentEntry.patientId"/></p> <p></urn4:Name></p> <p></urn4:ExternalIdentifier></p> <p>For submissions to PERM RC (since there is no ClaimId value), HIHs/providers shall submit the value of "NA" in the HL7 composite format as follows:</p> <p><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA^^^&amp;2.16.840.1.113883.13.34.110.1.200.2&amp;ISO" ></p> <p><urn4:Name></p> <p><urn4:LocalizedString value="XSDSDocumentEntry.patientId"/></p> <p></urn4:Name></p> <p></urn4:ExternalIdentifier></p>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
9. Cont 4	No additional information	<p>Note 4: To enable backward compatibility, HIHs/providers can also submit this patientID metadata attribute with the esMDClaimId value of 'NA' in standard format (i.e., no HL7 composite format):</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA" > <urn4:Name> <urn4:LocalizedString value="XSDSDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
10.	sourceId	<p>Globally unique identifier, in OID format, identifying the Health Information Handler (HIH) Gateway through which document/s are being sent to the CMS the esMD Gateway.</p> <pre><urn4:ExternalIdentifier id="ei04" registryObject="SubmissionSet01" identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832" value="12.16.840.1.113883.13.34.110.2"> <urn4:Name> <urn4:LocalizedString value="XDSSubmissionSet.sourceId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	HIH OID	String (64)
11.	submissionTime	<p>Point in Time when the SubmissionSet was created at the HIH CONNECT Adapter.</p> <pre><urn4:Slot name="submissionTime"> <urn4:ValueList> <urn4:Value>20041225235050</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Timestamp	Date (YYYYMMDDHMMSS)

No.	esMD XDR Submission Set Metadata Attribute	Definition and Example	R/R2/O/NR ADR, First Level Appeal Requests, Second Level Appeal Requests RA Discussion	R/R2/O/NR ADR to PERM	R/R2/O/NR PA, ADMC, X12 XDR (CTCs 12 & 13)	Metadata Attribute as per the Following Standard	References to the esMD Domain Specific Values	XDR Value - Data Type (Length)
12.	Title	<p>Represents the title of the Submission Set. The esMD Title for the Document SubmissionSet will be – ‘Claim Supporting Medical Documentation’.</p> <pre><urn4:Name> <urn4:LocalizedString value="Claim Supporting Medical Documentation"/> </urn4:Name></pre>	O	O	O	IHE ITI TF Rel. 6 Vol.3	Text	String (256)
13.	unique ID	<p>A globally unique identifier, in OID format, assigned by the HIH to the submission set in the transmission. The length of this Unique Identifier will not exceed 128 bytes.</p> <pre><urn4:ExternalIdentifier id="ei05" registryObject="SubmissionSet01" identificationScheme="urn:uuid:96fdda7c-d067-4183-912e- bf5ee74998a8" value="554ac39e-ef6343434-b233- 965d34345555"> <urn4:Name> <urn4:LocalizedString value="XDSSubmissionSet.uniqueId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Unique Identifier will not exceed 128 bytes	TBD

Table 6: The esMD Document Metadata Attributes details the esMD specific Document Metadata Attributes to confirm with the IHE ITI Technical Framework, Volume 3, Revision 6 and XDR Interoperability Testing.

Note: The following table indicates if the esMD XDR Document metadata attributes are required (R), XML Element Not Required (NR), required if known (R2), optional (O) To confirm IHE XDR interoperability test, add xml tag with the value as “NA”, if R2 or Optional.

Table 6: The esMD Document Metadata Attributes

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
1.	Author	<p>Represents the provider NPI or institution NPI who authored the individual Document included in the Submission Set</p> <p>This attribute contains either the following sub-attributes and never both:</p> <p>authorInstitution</p> <p>authorPerson</p> <pre> <urn4:Classification id="cl01" classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classifiedObject="Document01" nodeRepresentation="author"> <urn4:Slot name="authorInstitution"> <urn4:ValueList> <urn4:Value>603111</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Slot name="authorPerson"> <urn4:ValueList> <urn4:Value>603</urn4:Value> </urn4:ValueList> </urn4:Slot> </urn4:Classification> </pre>	R2	R2	R2	IHE ITI TF Rel. 6 Vol.3	Refer to Table 4.1-5 Document Metadata Attribute Definition in IHE ITI TF Volume 3 Revision 6.0 (http://www.ihe.net/Technical_Framework/upload/IHE_ITI_FT_6-0_Vol3_FT_2009-08-10-2.pdf)	Numeric (10)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
1.1.	authorInstitution (sub-attribute of author)	<p>Represents the NPI of the institution or the organization under which the human or machine authored the individual document included in the SubmissionSet.</p> <p>Note: At the Document Metadata level, either the authorInstitution or the authorPerson attribute will be used but never both.</p> <pre> <urn4:Slot name="authorInstitution"> <urn4:ValueList> <urn4:Value>604</urn4:Value> </urn4:ValueList> </urn4:Slot> </pre>	R2	R2	R2	IHE ITI TF Rel. 6 Vol.3	Institution NPI of the provider	Numeric (10)
1.2.	authorPerson (sub-attribute of author)	<p>Represents the NPI of the provider who authored the individual document included in the SubmissionSet.</p> <p>Note: At the Document Metadata level, either the authorInstitution or the authorPerson attribute will be used but never both.</p> <pre> <urn4:Slot name="authorPerson"> <urn4:ValueList> <urn4:Value>603</urn4:Value> </urn4:ValueList> </urn4:Slot> </pre>	R2	R2	N/A	IHE ITI TF Rel. 6 Vol.3	Document author NPI	Numeric (10)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
2.	classCode	<p>The code specifying the particular kind of document.</p> <pre><urn4:Classification id="cl02" classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a" classifiedObject="Document01" nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name="classCode"> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="See Table 7: ClassCodes and Corresponding ClassCode Display Names in this Implementation Guide" /> </urn4:Name> </urn4:Classification></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	See Table 7: ClassCodes and Corresponding ClassCode Display Names in this Implementation Guide	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
3.	classCode DisplayName	The name to be displayed for communicating to a human the meaning of the classCode. Will have a single value for each value of classCode used <urn4:Name> <urn4:LocalizedString value= "See Table 7: ClassCodes and Corresponding ClassCode Display Names in this Implementation Guide " /> </urn4:Name>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Refer to Table 7: ClassCodes and Corresponding ClassCode Display Names in this Implementation Guide	String (256)
4.	Comments	Comments associated with the Document in a free form text format <urn4:Description> <urn4:LocalizedString value="esMD Claim Document Submission in response to Review Contractor ADR Letter" /> </urn4:Description>	O	O	O	IHE ITI TF Rel. 6 Vol.3		String (256)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
5.	confidentialityCode	<p>The code specifying the level of confidentiality of the Document.</p> <p>For the esMD, the value is always 'V':</p> <pre><urn4:Classification id="cl03" classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedObject="Document01" nodeRepresentation="2.16.840.1.113883.5.25"> <urn4:Slot name="confidentialityCode"> <urn4:ValueList> <urn4:Value>V</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="VeryRestricted"/> </urn4:Name> </urn4:Classification></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Refer to Table 9: Confidentiality Codes in this Implementation Guide	String (64)
6.	creationTime	<p>Represents the time the HIH created the document.</p> <pre><urn4:Slot name="creationTime"> <urn4:ValueList> <urn4:Value>20110101165910</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Timestamp (DTM). HIH XDR created/submitted timestamp.	Date (YYYYMMDDHHMMSS)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
7.	entryUUID	<p>A unique ID or a globally unique identifier for each document in the Submission Set</p> <p>In the below example "Document01" is used as entryUUID. This can also be UUID format.</p> <p>Example:</p> <pre><urn4:ExtrinsicObject id="Document01" mimeType="application/pdf" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"> </urn4:ExtrinsicObject></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Unique Name for each attached document with a submitted document. Either UUID or some unique identifier.	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
8.	formatCode	<p>Globally unique code for specifying the format of the document. For example, the format code for the esMD is HITSP C62 urn:hitasp:c62:cda:pdf.</p> <pre> <urn4:Classification id="cl05" classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name="formatCode"> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="see description from Table 12: Document Format Code and Payload Type "/> </urn4:Name> </urn4:Classification> </pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	See Table 12: Document Format Code and Payload Type in this Implementation Guide	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
9.	Hash	Hash key of the XDR payload – C62 Document attachment based on the SHA1 Hash Algorithm <pre> <urn4:Slot name="hash"> <urn4:ValueList> <urn4:Value>ad18814418693512b767676006a21d8ec7291e84</urn4:Value> > </urn4:ValueList> </urn4:Slot> </pre>	R	R	R	IHE ITI TF Rel. 6 Vol3	SHA1 hash	String (256)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
10.	healthcareFacility TypeCode	<p>This code represents the type of organizational, provider setting of the claim or clinical encounters, or during which the documented act occurred.</p> <p>Note: If the submission request happens to be a response to an ADR letter, an Appeal, a RA Discussion Request, an ADCM Request, (PMD) PA Request, a Non-Emergent Ambulance Transport PA Request, or a_HBO PA Request, the healthcareFacility TypeCode with the value of either a 1 (which represents an HIH) or a 2 (which represents a provider) can be used. Please refer to Table 10: HealthCare Facility Type Code for HealthCare Facility Type Code information.</p> <pre> <urn4:Classification id="cl05" classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name=" healthcareFacilityTypeCode"> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="see description from table"/> </urn4:Name> </urn4:Classification> </pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Refer to Table 10: HealthCare Facility Type Code in this Implementation Guide	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
11.	healthcareFacilityTypeCodeDisplay Name	<p>The name to be displayed for communicating to a human the meaning of the healthcareFacilityTypeCode. Will have a single value corresponding to the healthcareFacilityTypeCode.</p> <pre> <urn4:Classification id="cl05" classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name=" healthcareFacilityTypeCode "> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="see description from table"/> </urn4:Name> </urn4:Classification> </pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	Refer to Table 10: HealthCare Facility Type Code in this Implementation Guide	String (128)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
12.	languageCode	<p>Specifies the human language of character data in the document. The values of the attribute are language identifiers as described by the IETF (Internet Engineering Task Force) RFC 3066.</p> <pre><urn4:Slot name="languageCode"> <urn4:ValueList> <urn4:Value>en-us</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	The esMD value may be "en-us"	String (16)
13.	mimeType	<p>MIME type of the document.</p> <pre><urn4:ExtrinsicObject id="Document01" mimeType="application/pdf" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"> </urn4:ExtrinsicObject></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	<p>The esMD PDF mimeType value shall be only "application/pdf" for PDF documents</p> <p>Note: Mime type is case sensitive.</p>	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
14.	patientID	<p>As per XDR specification, this patientID metadata attribute is mandatory. At this moment, the esMD does not handle patientID.</p> <p>For ADR, First Level Appeal Requests, Second Level Appeal Requests , RA Discussion Requests, and ADMC Requests use case submissions, HIHs/providers need to submit the esMDClaimId value in this patientID metadata attribute as follows:</p> <p>The ClaimId value needs to be sent in the HL7 composite format as mentioned under the esMDClaimId metadata attribute:</p> <p>Note 1: The '&' character must be properly (like &amp;) encoded in the XML content.</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="1234567890123^^^&amp;2.16.840.1.113883.13.34&amp;ISO"> <urn4:Name> <urn4:LocalizedString value="XSDSDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	The esMD value may be "NA"	HL7 CX Data type with String (256)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
14. Cont 1	No additional information	<p>Note 2: To enable backward compatibility, HIHs/providers may submit this patient metadata attribute with the esMDClaimId value in standard format (No HL7 composite format) as follows:</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="1234567890123"> <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre> <p>For Power Mobility, Non-Emergent Ambulance Transport, Hyperbaric Oxygen PA submissions, DMEPOS, and HHPCR demonstrations requests (since there is no ClaimID value), HIHs/providers may submit the value of "NA" in the HL7 composite format as follows:</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA^^^&amp;2.16.840.1.113883.13.34&amp;ISO" > <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
14. Cont. 2	No additional information	<p>Note 3: To enable backward compatibility, HIHs/providers may submit this patientId metadata attribute with the esMDClaimId value in standard format (No HL7 composite format):</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA" > <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre> <p>For submissions to PERM RC (since there is no ClaimId value), HIHs/providers shall submit the value of "NA" in the HL7 composite format as follows:</p> <pre><urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA^^^&amp;2.16.840.1.113883.13.34.110.1.200.2&amp;ISO" > <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
14. Cont. 3	No additional information	<p>Note 4: To enable backward compatibility, HIHs/providers can also submit this patientID metadata attribute with the esMDClaimId value of 'NA' in the standard format (i.e., no HL7 composite format).</p> <pre> <urn4:ExternalIdentifier id="ei03" registryObject="Document01" identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" value="NA" > <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.patientId"/> </urn4:Name> </urn4:ExternalIdentifier> </pre>	No additional information	No additional information	No additional information	No additional information	No additional information	No additional information

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
15.	practiceSetting Code	<p>The code specifying the clinical specialty where the act that resulted in the document was performed.</p> <p>This value will not be used by the esMD (i.e., will be ignored). However, since this field is required by XDR, an input is required.</p> <p>Not applicable to the esMD but required by XDR Interoperability.</p> <pre><urn4:Classification id="cl07" classificationScheme="urn:uuid:cccc5598-8b07-4b77-a05e-ae952c785ead" classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name="practiceSettingCode"> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="Practice Settings Code description"/> </urn4:Name> </urn4:Classification></pre>	R	R	R	IHE ITI TF Rel.6 Vol.3	The esMD value may be "1".	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
16.	practiceSettingCode DisplayName	<p>The name to be displayed for communicating to a human the meaning of the practiceSettingCode. Will have a single value corresponding to the practiceSettingCode.</p> <p>This value will not be used by the esMD (i.e., will be ignored). However, since this field is required by XDR, an input is required. Any possible value assigned by the sender will be accepted.</p> <pre><urn4:Name> <urn4:LocalizedString value="NA"/> </urn4:Name></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	The esMD value may be "NA".	String (64)
17.	serviceStartTime	<p>Represents the start time of the provider service being documented.</p> <p>This value will not be used by the esMD (i.e., will be ignored). However, since this field is required by XDR, an input is required. Any possible value assigned by the sender will be accepted.</p> <p>Not applicable to the esMD but required by XDR Interoperability.</p> <pre><urn4:Slot name="serviceStartTime"> <urn4:ValueList> <urn4:Value>20110101165910</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	<p>DateTimeStamp (HL7 V2 DTM).</p> <p>To pass the Interoperability Test – entry HIH submitted timestamp.</p>	Date (YYYYMMDDHHMMSS)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
18.	serviceStopTime	<p>Represents the stop time of the provider service being documented.</p> <p>This value will not be used by the esMD (i.e., will be ignored). However, since this field is required by XDR, an input is required. Any possible value assigned by the sender will be accepted.</p> <pre><urn4:Slot name="serviceStopTime"> <urn4:ValueList> <urn4:Value>20110101165910</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	DateTimeStamp (HL7 V2 DTM). To pass the Interoperability Test – entry HIH submitted timestamp.	Date (YYYYMMDDHHMMSS)
19.	Size	<p>Size in bytes of the C62 attachment byte stream that was provided through the request.</p> <p>Note: It is strongly recommended that HIHs/providers send the correct size of the payload.</p> <pre><urn4:Slot name="size"> <urn4:ValueList> <urn4:Value>1024000</urn4:Value> </urn4:ValueList> </urn4:Slot></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	In Bytes	Numeric (10,2)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
20.	Title	<p>Represents the title of the document. Max length, 128 bytes, UTF-8.</p> <pre><urn4:ExtrinsicObject id="Document01" mimeType="application/pdf" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"> <urn4:Name> <urn4:LocalizedString value="Get value from Table 11: Submission Set/Document Title"/> </urn4:Name> </urn4:ExtrinsicObject></pre>	O	O	O	IHE ITI TF Rel. 6 Vol.3	Possible Titles – Refer to Table 11: Submission Set/Document Title in this Implementation Guide No validation for this Title	String (256)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
21.	typeCode	<p>The code specifying the precise kind of document (e.g., Lab Order, Progress Notes, Orders).</p> <p>Note: The codes for typeCode metadata element are not defined yet for the esMD. HIHs/providers can send the value of '1' as mentioned in the example below.</p> <p>Also, note that typeCode (a document level metadata element) is different from ContentType code (a submission set metadata element).</p> <pre><urn4:Classification id="cl07" classificationScheme=" urn:uuid:f0306f51-975f-434e-a61c-c59651d33983 " classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name=" codingScheme "> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="Progress Note"/> </urn4:Name> </urn4:Classification></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3		String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
22.	typeCodeDisplay Name	<p>The name to be displayed for communicating to a human the meaning of the typeCode. Will have a single value for each value of typeCode.</p> <p>Note: Since the typeCodes are not yet defined for the esMD as noted in row 21 of this table (see above), the type CodeDisplay name can have any appropriate name.</p> <pre> <urn4:Classification id="cl07" classificationScheme=" urn:uuid:f0306f51-975f-434e-a61c-c59651d33983 " classifiedObject="Document01" nodeRepresentation=" 2.16.840.1.113883.13.34.110.1.1000.1"> <urn4:Slot name=" codingScheme "> <urn4:ValueList> <urn4:Value>1</urn4:Value> </urn4:ValueList> </urn4:Slot> <urn4:Name> <urn4:LocalizedString value="Progress Note"/> </urn4:Name> </urn4:Classification> </pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3		String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
23.	legalAuthenticator	<p>The authenticator of the document at the provider.</p> <pre><urn4:slot name="legalAuthenticator"> <urn4:ValueList> <urn4:Value>NA</urn4:Value> </urn4:ValueList> </urn4:slot></pre>	O	O	O	IHE ITI TF Rel. 6 Vol.3	NA	String (32)
24.	uniqueId	<p>A globally unique identifier assigned by the HIH to each document in the SubmissionSet. The length of the Unique Identifier will not exceed 128 bytes. The structure and format of this ID will be consistent with the specification corresponding to the format attribute. This ID will be generated based on the UUID. The same ID will be returned with the response message.</p> <pre><urn4:ExternalIdentifier id="ei02" registryObject="Document01" identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8" value="1.3.6.1.4.1.21367.2005.3.9999.33"> <urn4:Name> <urn4:LocalizedString value="XSDDocumentEntry.uniqueId"/> </urn4:Name> </urn4:ExternalIdentifier></pre>	R	R	R	IHE ITI TF Rel. 6 Vol.3	UUID Refer to ITI TF 4.1.7.2 Volume 3 Revision 6	String (64)

No.	The esMD XDR Submission Set Setadata Attribute	Definition and Example	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests Non-Perm	R/R2/O ADR First Level Appeal Requests, Second Level Appeal Requests RA Discussion Requests ADMC Requests PERM	R/R2/O PA X12 XDR (CTCs 12 & 13)	Metadata Attribute as per Following Standard	References to a Possible esMD Domain Specific Value	XDR Value -Data Type (Length)
25	Attachment Control Number	<p>Identification number provided by the requester in PWK06 segment if the requester has additional documentation associated with the health services review that applies to the service requested.</p> <p>This is used to associate a X12N 278 5010 request with the supporting documentation received in the XDR format.</p> <p>This applies to Content Type Code 12 and 13.</p>			R			

5.3.39 Attachment Control Number (ACN)

The Attachment Control Number received originally on an EDI X12 278 5010 request is stored in the esMD database. The supporting documentation submitted in XDR format should include same Attachment Control Number (ACN) as the original EDI X12N 278 5010 request in order for the esMD to associate the request with its supporting documentation. As soon as the documentation is received the esMD locates the EDI X12N 278 5010 request in the esMD database using the Attachment Control Number. Once the matching request and documentation is found having the same Attachment Control Number and NPI combination, the esMD packages the request and the documentation together in order to forward it to the Review Contractor.

5.3.40 Intended Recipients

The HIH should provide the receiving RC's OID as the value for Intended Recipient field. For more information on the RC OIDs, Sender IDs, refer to the link below:

http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which_Review_Contractors_Accept_esMD_Transactions.html

Note 1: From the implementation of the esMD R3.1, a validation has been put in place to check whether a specific RC accepts a particular Content Type Code. If a RC does not accept a specific use case (Content Type Code), then the submission will be rejected. Please refer to the following CMS Government website in the download section for the updated list of Review Contractors and the lines of business accepted by each RC: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which_Review_Contractors_Accept_esMD_Transactions.html.

5.3.41 Content Type Code

The Content Type Code with the value of "1", response to ADR Letter is accepted by all RCs participating in the esMD.

The Content Type Code with the value of "8" shall be used for Power Mobility Device (PMD) Prior Authorization PA request submissions. Only DME MACs A, B, C, and D accept such PA requests from providers. For more details, please visit the following website: <http://go.cms.gov/PADemo>.

The esMD supports the following Prior Authorization programs. These PA Programs will be utilized by the A/B MACs only:

1. The Content Type Code with a value of "8.1" is used for Repetitive Scheduled Non-Emergent Ambulance Transport Prior Authorization requests. Novitas and Palmetto are accepting this line of business.
2. The Content Type Code with a value of "8.2" is used for Hyperbaric Oxygen Prior Authorization requests. NGS, WPS, and Novitas are accepting this line of business.

Refer to the Table 8: Content Type Codes and Corresponding Content Type Code Display Names for more details on the Content Type Codes supported by the esMD.

Please refer to the following link for CMS Government website for the updated list of lines of businesses accepted by each RC:

http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Which_Review_Contractors_Accept_esMD_Transactions.html.

Table 7: ClassCodes and Corresponding ClassCode Display Names provides the ClassCodes and corresponding ClassCode Display Names.

Metadata Vocabulary - Class Schema: urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a

Table 7: ClassCodes and Corresponding ClassCode Display Names

Class Code	Class Code Display Name	Coding Schema / Code System
1	Unstructured	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
2	Structured	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema

Table 8: Content Type Codes and Corresponding Content Type Code Display Names provides the Content Type Codes and Corresponding Content Type Code Display Names.

Metadata Vocabulary - Class Schema: urn:uuid:f0306f51-975f-434e-a61c-c59651d33983

Table 8: Content Type Codes and Corresponding Content Type Code Display Names

Content Type Code	Content Type Code Display Name	Coding Schema / Code System
1	Response to Additional Documentation Request (ADR)	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
8	Power Mobility Device (PMD) Prior Authorization (PA) Requests	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
8.1	Non-Emergent Ambulance Transport PA Request	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
8.2	Hyperbaric Oxygen PA Request	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
9	First Level Appeal Requests	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
9.1	Second Level Appeal Requests	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema

Content Type Code	Content Type Code Display Name	Coding Schema / Code System
10	Advance Determination of Medicare Coverage (ADMC) Request	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
11	RA Discussion Requests	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
12	Supporting Documentation for the unsolicited X12N 278 5010 Request in XDR format. Note: Original X12N 278 5010 request for this supporting documentation is not tracked through the esMD system.	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema
13	Unsolicited X12N 278 5010 Request in CAQH format tracked through the esMD system.	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Schema

The Content Type Code Display Name column in Table 8: Content Type Codes and Corresponding Content Type Code Display Names represent the lines of business for the CMS. The esMD accepts documentation from providers and HIHs.

Table 9: Confidentiality Codes provides the Confidentiality Codes.

Metadata Vocabulary - Class Schema: urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f

Reference URL: <http://xml.coverpages.org/CDA-Release2-Unofficial.html>.

Table 9: Confidentiality Codes

Confidentiality Code	Description	Coding Schema / Code System
N	Normal	2.16.840.1.113883.5.25
R	Restricted	2.16.840.1.113883.5.25
V *	Very Restricted (default for the esMD)	2.16.840.1.113883.5.25

* The esMD will only accept the Very Restricted Confidentiality Code.

Table 10: HealthCare Facility Type Code provides the HealthCare Facility Type Codes.

Metadata Vocabulary - Class Schema: urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1

Table 10: HealthCare Facility Type Code

Type Code	HealthCare Facility Type Code Display Name	Coding Schema / Code System
1.	Health Information Handler (HIH)	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Class Codes
2.	Health Care provider	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Class Codes
3.	The CMS Review Contractor	2.16.840.1.113883.13.34.110.1.1000.1 - CMS Class Codes

Table 11: Submission Set/Document Title provides the Submission Set or Document Title.

Table 11: Submission Set/Document Title

Submission Set/Document Title
Solicited Supporting Documentation
Additional Documentation Request
Unsolicited Documentation

Table 12: Document Format Code and Payload Type provides the Document Format Code and Payload Type.

Metadata Vocabulary - Class Schema: urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d

Table 12: Document Format Code and Payload Type

No.	Format Code	Format Description	Coding Schema / Code System
1.	HITSP C62 urn:hitsp:c62:cda:pdf	Scanned PDF Document in Clinical Document Architecture (CDA) C62 Construct	2.16.840.1.113883.13.34.110.1.1000.1 – The esMD Schema
2.	HITSP C62 urn:hitsp:c62:cda:tiff	Scanned TIFF Document in CDA C62 Construct	2.16.840.1.113883.13.34.110.1.1000.1 – The esMD Schema
3.	HITSP C83	HITSP C83	2.16.840.1.113883.13.34.110.1.1000.1 - The esMD Schema
4.	HITSP C32	HITSP C32	2.16.840.1.113883.13.34.110.1.1000.1 - The esMD Schema

No.	Format Code	Format Description	Coding Schema / Code System
5.	urn:ihe:iti:xds-sd:pdf:2008	Scanned PDF Document in XDS	1.3.6.1.4.1.19376.1.2.3
6.	urn:ihe:iti:xds-sd:text:2008	Scanned Documents with text (XDS-SD)	1.3.6.1.4.1.19376.1.2.3

Table 13: Overall Mapping of Document Submission with Class and Content Type Codes details the Overall Mapping of the Document Submission with the Class and Content Type Codes.

This table shows the possible combinations/mappings between Unsolicited and Solicited Documentation, Format Code, Class Code, and Type Code.

Table 13: Overall Mapping of Document Submission with Class and Content Type Codes

Solicited Supporting and Unsolicited Documentation	FormatCode (Payload Construct)	ClassCode	Class Code Display Name	Content Type Code	Content Type Code Display Name
Solicited Supporting Documentation	HITSP C62	1	Unstructured	1	Response to Additional Documentation Request (ADR)
Unsolicited Documentation	HITSP C62	1	Unstructured	8	Power Mobility Device (PMD) Prior Authorization (PA) Request
Unsolicited Documentation	HITSP C62	1	Unstructured	8.1	Non-Emergent Ambulance Transport PA Request
Unsolicited Documentation	HITSP C62	1	Unstructured	8.2	Hyperbaric Oxygen PA Request
Unsolicited Documentation	HITSP C62	1	Unstructured	9	First Level Appeal Requests
Unsolicited Documentation	HITSP C62	1	Unstructured	9.1	Second Level Appeal Requests
Unsolicited Documentation	HITSP C62	1	Unstructured	10	Advance Determination of Medicare Coverage

Solicited Supporting and Unsolicited Documentation	FormatCode (Payload Construct)	ClassCode	Class Code Display Name	Content Type Code	Content Type Code Display Name
Unsolicited Documentation	HITSP C62	1	Unstructured	11	RA Discussion Requests
Unsolicited Documentation	HITSP C62	1	Unstructured	12	Supporting Documentation for the unsolicited X12N 278 Request in XDR format.
Unsolicited Supporting Documentation	HITSP C62	1	Unstructured	13	Unsolicited X12N 278 Request in CAQH format tracked the through esMD system.

Note: Table 14: Combination of the esMD Codes and Claim/Case IDs for Different Types of Submission Requests presents the possible values that will be accepted. If the values sent by the HIH/provider do not match for the corresponding type of submission request, the submission will be rejected. As of Release 3.1, the Claim Id is optional for First Level Appeal Requests

Table 14: Combination of the esMD Codes and Claim/Case IDs for Different Types of Submission Requests

No.	Type of Submission Request	Content Type Code (Submission Set Metadata Attribute)	HealthCare Facility Type Code (Document Metadata Attribute)	Format Code (Document Metadata Attribute)	Class Code (Document Metadata Attribute)	The esMDClaimId (SubmissionSet Metadata Attribute)	The esMDCaseld (SubmissionSet Metadata Attribute)	The AttachmentControlNumber (SubmissionSet Metadata Attribute)
1.	Response to ADR	1	1, 2	1	1	Required	Required if known	N/A
2.	Power Mobility Device PMD Prior Authorization (PA) Request	8	1, 2	1	1	No. TheesMDClai mId xml metadata attribute tag should not be provided	No. The esMDCaseld xml metadata attribute tag should not be provided	N/A

No.	Type of Submission Request	Content Type Code (Submission Set Metadata Attribute)	HealthCare Facility Type Code (Document Metadata Attribute)	Format Code (Document Metadata Attribute)	Class Code (Document Metadata Attribute)	The esMDClaimId (SubmissionSet Metadata Attribute)	The esMDCaseld (SubmissionSet Metadata Attribute)	The AttachmentControlNumber (SubmissionSet Metadata Attribute)
3.	First Level Appeal Requests	9	1, 2	1	1	Optional	Optional	N/A
3.1	Second Level Appeal Requests	9.1	1,2	1	1	Optional	Optional	N/A
4.	Advance Determination of Medicare Coverage	10	1, 2	1	1	Required	Required if known	N/A
5.	RA Discussion Requests	11	1, 2	1	1	Required	Required if known	N/A
6	Supporting Documentation for the unsolicited X12N 278 5010 Request	12	1, 2	1	1	No. The esMD ClaimID xml metadata attribute tag should not be provided	No. The esMD systemCaseld xml metadata attribute tag should not be provided	Required
7.	Supporting Documentation for the X12N 278 5010 Request	13	1, 2	1	1	No. The esMD ClaimID xml metadata attribute tag should not be provided	No. The esMD systemCaseld xml metadata attribute tag should not be provided	Required

No.	Type of Submission Request	Content Type Code (Submission Set Metadata Attribute)	HealthCare Facility Type Code (Document Metadata Attribute)	Format Code (Document Metadata Attribute)	Class Code (Document Metadata Attribute)	The esMDClaimId (SubmissionSet Metadata Attribute)	The esMDCaseld (SubmissionSet Metadata Attribute)	The AttachmentControlNumber (SubmissionSet Metadata Attribute)
8.	Non-Emergent Ambulance Transport Prior Authorization Requests	8.1	1, 2	1	1	No. The esMDClaimId xml metadata attribute tag should not be provided	No. The esMDCaseld xml metadata attribute tag should not be provided	N/A
9.	Hyperbaric Oxygen Prior Authorization Requests	8.2	1, 2	1	1	No. The esMDClaimId xml metadata attribute tag should not be provided	No. The esMDCaseld xml metadata attribute tag should not be provided	N/A

5.3.42 HITSP C62 (Construct on Top of CDA) Document Constraints

This section outlines the content of the unstructured HITSP C62 Construct (on top of the HL7 CDA) constraints for the document. The requirements specified below are to ensure the presence of a minimum amount of wrapper data in order to enhance description and facilitate submitting the claim documentation.

```
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" classCode="DOCCLIN" moodCode="EVN" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">
  <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
```

```
<id root="eab8765b-1424-47cc-9495-ddc934cf5f5d"/>
```

```
<templateId root="2.16.840.1.113883.10.20.3" assigningAuthorityName="CDT General Header Constraints"/>
```

```
<templateId root="1.3.6.1.4.1.19376.1.5.3.1.1.1" assigningAuthorityName="IHE Medical Document"/>
```

```
<templateId root="1.3.6.1.4.1.19376.1.2.20" assigningAuthorityName="IHE Scanned Document"/>
```

```
<templateId root="2.16.840.1.113883.3.88.11.62.1" assigningAuthorityName="HITSP Unstructured Document"/>
```

```
<languageCommunication>
```

```

<templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.1'/>
<languageCode code='en-US'/>
</languageCommunication>
<title>ADR Response Supported Claim Documentation</title>
<confidentialityCode code="V" codeSystem="2.16.840.1.113883.5.25"
codeSystemName="Confidentiality" displayName="Very Restricted"/>
<effectiveTime value="20100319083838-0500"/>

  <recordTarget>
    <patientRole>
      <id extension="12345" root="2.16.840.1.113883.3.933"/>
      ...
    </patientRole>
  </recordTarget>
  <author>
    <templateId root="1.3.6.1.4.1.19376.1.2.20.1"/>
    ...
  </author>
  <author>
    <templateId root="1.3.6.1.4.1.19376.1.2.20.2"/>
    ...
  <dataEnterer>
    <templateId root="1.3.6.1.4.1.19376.1.2.20.3"/>
    ...
  </dataEnterer>
  <custodian>
    ...
  </custodian>
  <legalAuthenticator>
    ...
  </legalAuthenticator>
</documentationOf>
  <serviceEvent >
    <effectiveTime>
      <low value="19800127"/>
      <high value="19990522"/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
<component>
  <nonXMLBody>
    <text mediaType="application/pdf" representation="B64">

```

```
JVBERi0xLjMKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFlvRmlsdGVyIC9GbGF0
</text>
</nonXMLBody>
</component>
</ClinicalDocument>
```

Table 15: CDA Document Constraints Specifications details the CDA Document Constraints Specifications.

Table 15: CDA Document Constraints Specifications

No.	HITSP C62 Construct → HL7 CDA Header Element	Description and Source / Value	R/R2/O	References to Possible the esMD Domain Specific Values
1.	ClinicalDocument/typeld	Fixed, per CDA version in use. <typeld extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>	R	
2.	ClinicalDocument/templated	This element will be present. The root attribute will contain the OID, '2.16.840.1.113883.3.88.11.62.1', to indicate what type of document is an XDR document. <templated root="2.16.840.1.113883.10.20.3" assigningAuthorityName="CDT General Header Constraints"/> <templated root="1.3.6.1.4.1.19376.1.5.3.1.1.1" assigningAuthorityName="IHE Medical Document"/> <templated root="1.3.6.1.4.1.19376.1.2.20" assigningAuthorityName="IHE Scanned Document"/> <templated root="2.16.840.1.113883.3.88.11.62.1" assigningAuthorityName="HITSP Unstructured Document"/>	R	
3.	ClinicalDocument/id	This element will be present. The root attribute will contain the OID, which Represents the unique instance identifier of a clinical document. Computable. <id root="eab8765b-1424-47cc-9495-ddc934cf5f5d"/>	R	

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/ R2 /O	References to Possible the esMD Domain Specific Values
4.	ClinicalDocument/code	<p>Values for this code are dictated by the CDA R2 documentation, but are permissible to extend to fit the particular use case. Attributes code@code and code@codeSystem will be present.</p> <p>Entered by the operator, or possibly can be taken from the scanned content.</p> <pre><code="34133-9" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC" displayName="esMD Document Submission"/></pre>	R	
5.	ClinicalDocument/title	<p>This will be present if known.</p> <p>Entered by operator, or possibly can be taken from the scanned content.</p> <pre><title>ADR Response – Supported Claim Documentation</title></pre>	R2	
6.	ClinicalDocument/confidentialityCode	<p>Will be assigned by the operator in accordance with the scanning facility policy. The notion or level of confidentiality in the header may not be the same as that in the Affinity Domain, but in certain cases could be used to derive a confidentiality value among those specified by the Affinity Domain. Attributes confidentialityCode@code and confidentialityCode@codeSystem will be present.</p> <p>Assigned by the operator Computed. This is the scan time.</p> <pre><confidentialityCode code="V" codeSystem="2.16.840.1.113883.5.25" codeSystemName="Confidentiality" displayName="Very Restricted"/></pre>	R	Refer to Table 9: Confidentiality Codes

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/ R2 /O	References to Possible the esMD Domain Specific Values
7.	ClinicalDocument/effectiveTime	<p>This should denote the time at which the original content was scanned. Signifies the document creation time, when the document first came into being. At a minimum, the time will be precise to the day and will include the time zone offset from GMT.</p> <p>Computed. This is the scan time.</p> <pre><effectiveTime value="20050329224411+0500"/></pre>	R	
8.	ClinicalDocument/languageCode	<p>This element in accordance with the HL7 CDA R2 documentation specifies the human language of character data.</p> <p>Entered by operator</p> <pre><languageCommunication> <templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.1'/> <languageCode code='en-US'/> </languageCommunication></pre>	R	

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/R2/O	References to Possible the esMD Domain Specific Values
9.	ClinicalDocument/recordTarget	<p>The ClinicalDocument/recordTarget contains identifying information about the patient concerned in the original content.</p> <p>Taken from scanned content, supplemented by operator.</p> <pre> <recordTarget> <patientRole> <id extension="12345" root="2.16.840.1.113883.3.933"/> <addr> <streetAddressLine>NA</streetAddressLine> <city>NA</city> <state>NA</state> <postalCode>NA</postalCode> <country>NA</country> </addr> <patient> <name> <prefix>NA</prefix> <given>NA</given> <family>NA</family> </name> <administrativeGenderCode code="F" codeSystem="2.16.840.1.113883.5.1"/> <birthTime value="19600127"/> </patient> </patientRole> </recordTarget> </pre>	R	Data is optional for the esMD. If submitting, need to provide de-identified data or NA.

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/R2/O	References to Possible the esMD Domain Specific Values
10.	ClinicalDocument/author/assignedAuthor/assignedPerson	<p>This element represents the author of the original content. It additionally can 1040 encode the original author's institution in the sub-element represented Organization. Information regarding the original author and his/her institution should be included, if it is known.</p> <p>Taken from scanned content, supplemented by operator. This is the original author.</p> <pre> <author> <templateId root="1.3.6.1.4.1.19376.1.2.20.1"/> <time value="19990522"/> <assignedAuthor> <id extension="11111111" root="1.3.5.35.1.4436.7"/> <assignedPerson> <name> <prefix>NA</prefix> <given>NA</given> <family>NA</family> <suffix>NA</suffix> </name> </assignedPerson> <representedOrganization> <id extension="aaaaabbbb" root="1.3.5.35.1.4436.7"/> <name>NA</name> </representedOrganization> </assignedAuthor> </author> </pre>	R2	Data is optional for the esMD

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/R2/O	References to Possible the esMD Domain Specific Values
11.	ClinicalDocument/author/assignedAuthor/authoringDevice	<p>This element will be present and represent the scanning device and software used to produce the scanned content.</p> <p>Can be computed or fixed based on the scanning device and software. This is the information about the scanning device.</p> <p>97441496</p> <pre> <name>SOME Scanning Facility</name> <addr> <streetAddressLine>NA</streetAddressLine> <city>NA</city> <state>NA</state> <postalCode>NA</postalCode> <country>NA</country> </addr> </representedOrganization> </assignedAuthor> </author> </pre>	R	Data is optional for the esMD
12.	ClinicalDocument/dataEnterer	<p>This element represents the information about the scanner operator.</p> <pre> <dataEnterer> <templateId root="1.3.6.1.4.1.19376.1.2.20.3"/> <time value="20050329224411+0500"/> <assignedEntity> <id extension="22222222" root="1.3.6.4.1.4.1.2835.2"/> <assignedPerson> <name> <prefix>NA.</prefix> <given>NA</given> <family>NA</family> </name> </assignedPerson> </assignedEntity> </dataEnterer> </pre>	R	Data is optional for the esMD

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/ R2 /O	References to Possible the esMD Domain Specific Values
13.	ClinicalDocument/custodian	<p>Represents the HIH organization from which the document originates and that is in charge of maintaining the document. The custodian is the steward that is entrusted with the care of the document. Every CDA document has exactly one custodian. In most cases, this will be the scanning facility.</p> <pre> <custodian typeCode="CST"> <assignedCustodian classCode="ASSIGNED"> <representedCustodianOrganization classCode="ORG" determinerCode="INSTANCE"> <id root="1.300011"/> <name>QSSI INC.</name> <telecom use="WP" value="(555)555-5500"/> <addr> <streetAddressLine> 100 Governor Warfield Parkway</streetAddressLine> <city>Columbia</city> <state>MD</state> <postalCode>21044</postalCode> <country/> </addr> </representedCustodianOrganization> </assignedCustodian> </custodian> </pre>	R	Data related to HIH and in sync with the Submission set meta data.

No.	HITSP C62 Construct →HL7 CDA Header Element	Description and Source / Value	R/R2/O	References to Possible the esMD Domain Specific Values
14.	ClinicalDocument/documentationOf/serviceEvent/effectiveTime	<p>This element is used to encode the date/time range of the original content. If the original content is representative of a single point in time then the endpoints of the date/time range will be the same. Information regarding this date/time range should be included, if it is known. In many cases, this will have to be supplied by the operator.</p> <p>Denotes the time/date range of the original content.</p> <pre><documentationOf> <serviceEvent > <effectiveTime> <low value="19800127"/> <high value="19990522"/> </effectiveTime> </serviceEvent> </documentationOf></pre>	R	
15.	ClinicalDocument/component/nonXML Body	The scanned/base64 encoded content.	R	

The sending provider may be 1) the provider whose claim is in question, 2) the provider who orders the item on service listed on the claim in question, or 3) a provider who rendered a service related to the claim in question. HIHs may include the digital signature and date stamp associated with the medical record entry being transmitted. Though not required, HIHs may also list the Certification Commission for Health Information Technology (CCHIT) certification number associated with the medical record entry.

5.4 Content Type Codes

Table 16: Content Type Code Descriptions provides the Content Type Code descriptions.

Table 16: Content Type Code Descriptions

Content Type Code	Description	Comment
1	Response to Additional Documentation Request(ADR)	N/A
8	PMD PA	N/A
9	First Level Appeal Requests	N/A
9.1	Second Level Appeal Requests	N/A
10	ADMC	N/A
11	RA Requests	N/A
12	Supporting Documentation for the unsolicited X12N 278 5010 Request	N/A
13	Supporting Documentation for the X12N 278 5010 Request	N/A
8.1	Non-Emergent Ambulance Transport	N/A
8.2	Hyperbaric Oxygen (HBO) Therapy	N/A

6 XDR Validation

The following validations occur in the esMD for the inbound submission in XDR format:

1. TLS Authentication
2. OID Validation (Authorization) - Home Community OID Verification against the CMS Certified HIHs based on CMS Onboarding Process
3. Check Payload Size
4. A Copy of Payload is Sent to Blue Coat Gateway for Virus Scanning
5. Check for Duplicate Unique Identifier (ID)
6. Claim reviewer Participation Validation
7. Affinity Values validation
8. Document Availability in submission
9. Base64 SHA1 Decoding Validation for Payload attachments
10. Review Contractor and Content Type Code cross validation – this is to check whether a particular CMS RC accepts a particular document submission (e.g., PMD PAR, Response to ADR, First Level Appeal Requests and Second Level Appeal Requests., ADMC Request, RA Discussion Request, Non-Emergent Ambulance Transport Requests , Hyperbaric Oxygen Prior Authorization Requests , DMEPOS, and HHPCR demonstration requests).

7 XDR Error Messages

Table 17: Error Messages provides details for each error message and identifies the error messages currently used by the esMD Gateway.

Table 17: Error Messages

No.	Fatal Error Code	Discussion
1.	XDSHOIDidDoesNotMatch	The XDR specifies where the submitted HIH Home Community IDs must match between documents (i.e., submission sets and the esMD Onboarded HIH OID).
2.	XDSDuplicateUniqueIDInRegistry	The UniqueID received was not unique within the Registry. The UniqueID could have been attached to earlier XDSSubmissionSet.
3.	XDSMissingDocumentMetadata	The MIME package contains the MIME part with Content-ID header not found.
4.	XDSRegistryMetadataError	An Error was detected in the metadata. The Actor name indicates where the error was detected. The CodeContext indicates the nature of the problem. This error code will be used to convey validation related errors for the following: Class Code, Content Type Code, Format Code, HealthCare Facility Type code, Confidentiality Code, the esMDClaimId, the esMDCasId, and NPI. It will also be used to convey errors related to RC OID and Content Type Code cross validation.
5.	XDSMissingDocument	The Metadata exists with no corresponding attached document.
6	XDSNonIdenticalHash	The Hash code of the attached document does not match.
7	CMS DocumentVirus ScanError	Any Antivirus scan failures that occur in the process of delivery and at RC end.
8.	XDSRegistryError	Internal the esMD Registry/Repository Error
9.	XDSRegistryBusy	Too Much Activity

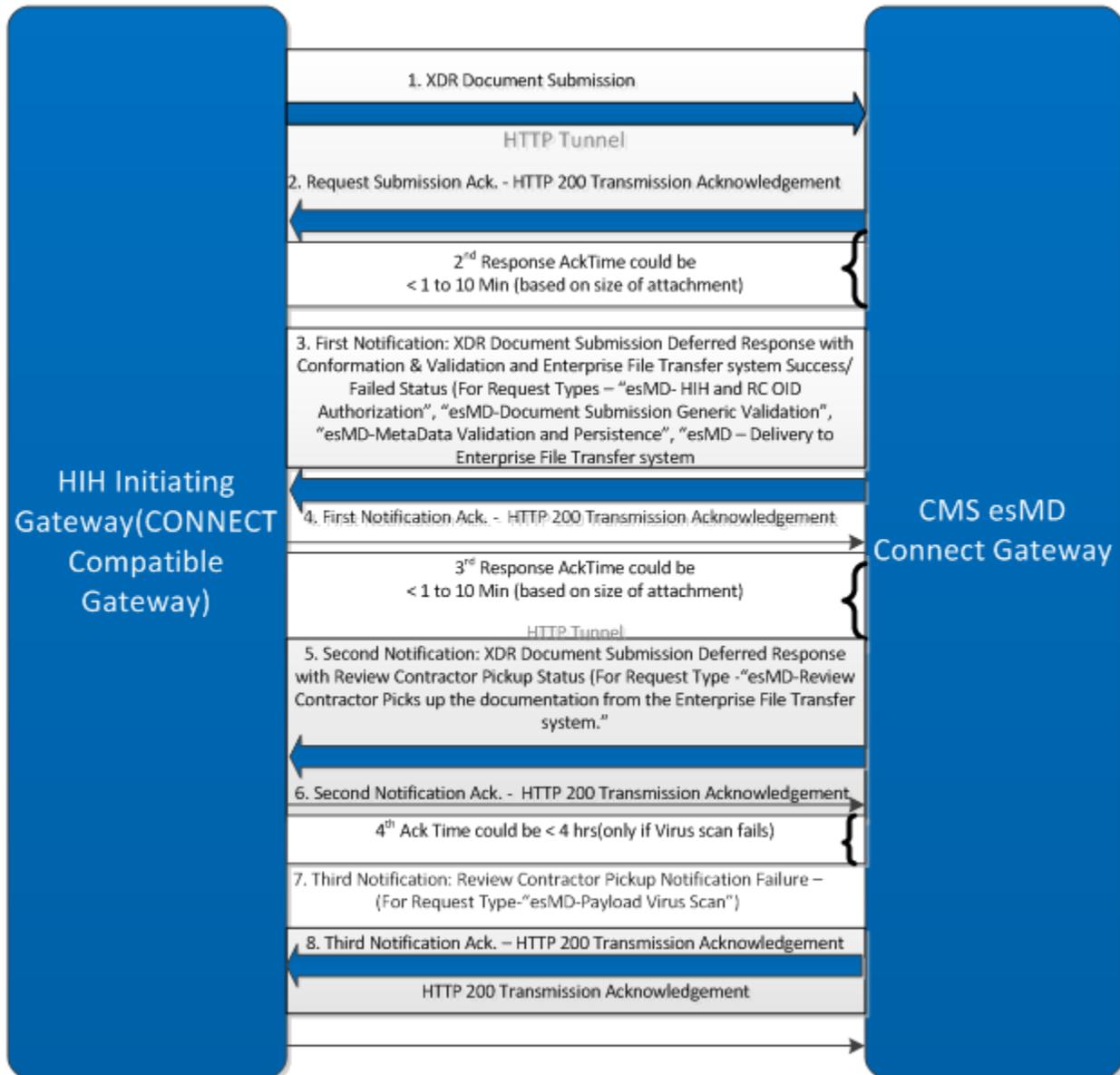
No.	Fatal Error Code	Discussion
10.	XDSRegistryOutOfResources	Resources are low
11.	RCAdministrativeError	Administrative Errors was received from RC. This error code will be used to convey RC Administrative related errors for the following: corrupt Files

* Warning messages will be considered as information and will not be categorized as fatal errors. No warning messages have been identified at this time.

8 XDR Status and Notification Messages

Refer to Figure 4: Document Submission Deferred Responses with Multiple HTTP Connections for the information discussed in this section.

Figure 4: Document Submission Deferred Responses with Multiple HTTP Connections



8.1 The esMD First Acknowledgment - HTTP Status Code

HIHs will take actions based on the HTTP Status code. The HTTP Status code of 200 indicates a successful submission while the HTTP status codes from 300 through 499 indicate the possibility of

a fatal error. The esMD Team expects HIHs to take appropriate action to fix fatal errors. The esMD specific HTTP Status codes series will begin from 500.

HTTP status codes are the codes that the client (HIH) Web server uses to communicate with the esMD Web browser or user agent.

The HTTP status codes will allow HIHs to control their Web server with a higher degree of accuracy and effectiveness.

Table 18: HTTP Status Codes indicates the category assigned to each HTTP Status Code numerical series.

Table 18: HTTP Status Codes

HTTP Status Code Series	Code Category
HTTP Status Codes 100-101	Informational Status Codes
HTTP Status Codes 200-206	Successful Status Codes
HTTP Status Codes 300-307	Redirection Status Codes
HTTP Status Codes 400-416	Client Error Status Codes
HTTP Status Codes 500-505	Server Error Status Codes

For more details, please visit: http://webdesign.about.com/od/http/a/http_status_codes.htm.

The XDR Deferred Document Submission Response SOAP message will have the Assertions, Target Communities (as HIH OID, Description, and Name), and Response.

To correlate the request to the response, the unique ID (AssertionType.getSamlAuthzDecisionStatement().getEvidence().getAssertion().getId()) and message ID will be copied back into the response message.

8.1.1 Success Message

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
```

```
<soap:Header>
```

```
<Action
```

```
xmlns="http://www.w3.org/2005/08/addressing">urn:ihe:iti:xdr:2007:XDRRequestAcknowledgementMessage</Action>
```

```
<MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:7a38905c-8235-400c-8c7a-bf96f5a12834</MessageID>
```

```

<To
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymous</To>

  <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">uuid:37f4ac23-da88-4fcb-8030-dd15d9835ded</RelatesTo>

  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" soap:mustUnderstand="true">

    <wsu:Timestamp wsu:Id="TS-131">

      <wsu:Created>2015-02-09T17:07:23.267Z</wsu:Created>

      <wsu:Expires>2015-02-09T17:12:23.267Z</wsu:Expires>

    </wsu:Timestamp>

    <wsse11:SignatureConfirmation xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
Value="SNkSuCQE5E9IGAOWSG5N3zxmewxC1m4YEFi70phOUeJO2l/3PZhF9FynZEUjI9C5DdVKoSS8eVmh/WqExC8dTSVZahSeSbwK+jxE484hTRJtT5gxnj7G4/5OkMmcxYDBkdILOyZNY6PmhmZ1RxAFNzNTPOCGrnbuFlceTg5FT8ERaNV4y/4CDlpRIPDYGt7AoQvhNINeBsjZgcFiSzUijFFtutxfK+Rvs/53aoyEDtXsGgw1Xf+HFGBAN+CjcNi/pHuk0HEIO1U8aLfiJqbYs1sAjiB+4YVDTwHyxsi2jdCBzww/w/V1fRZMF08sMauHhTjz9nyHmZK2H/zWV24w==" wsu:Id="SC-132"/>

  </wsse:Security>
</soap:Header>
<soap:Body>

  <ns6:XDRAcknowledgement xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0" xmlns:ns4="urn:ihe:iti:xds-b:2007" xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0" xmlns:ns6="http://www.hhs.gov/healthit/nhin">

    <ns6:message status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:RequestAccepted"/>

  </ns6:XDRAcknowledgement>
</soap:Body>
</soap:Envelope>

```

8.1.2 The esMD Error Messages

The error message below serves as a generic XDR error message example. Note the use of `errorCode` and `codeContext` below:

```

<ns2:RegistryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-

```

```
regrep:xsd:query:3.0" xmlns:ns4="http://www.hhs.gov/healthit/nhin"
xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0" requestId="esMD - Meta Data Validation
and Persistence" status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
```

```
<ns2:ResponseSlotList>
```

```
<Slot name="esMDTransactionId">
```

```
<ValueList>
```

```
<Value>1076321</Value>
```

```
</ValueList>
```

```
</Slot>
```

```
<Slot name="esMDClaimId">
```

```
<ValueList>
```

```
<Value>1234567890123</Value>
```

```
</ValueList>
```

```
</Slot>
```

```
<Slot name="esMDCasId">
```

```
<ValueList>
```

```
<Value>1234567890123</Value>
```

```
</ValueList>
```

```
</Slot>
```

```
<Slot name="contentTypeCode">
```

```
<ValueList>
```

```
<Value>9</Value>
```

```
</ValueList>
```

```
</Slot>
```

```
</ns2:ResponseSlotList>
```

```
<ns2:RegistryErrorList highestSeverity="urn:oasis:names:tc:ebxml-
regrep:ErrorSeverityType:Error">
```

<ns2:RegistryError codeContext=" THE ESMD_317 - The Review Contractor to whom this submission was sent does not accept this particular document, identified by the ContentType code. Please change either the Review Contractor OID or the ContentType Code and submit again"

```
errorCode="XDSRegistryMetadataError" severity="urn:oasis:names:tc:ebxml-
regrep:ErrorSeverityType:Error">
```

```
</ns2:RegistryError>
```

```
</ns2:RegistryErrorList>
</ns2:RegistryResponse>
```

8.2 The esMD System First Notification

8.2.1 Metadata Validation

Based on following validations, an asynchronous XDR Response message with success or detailed failed acknowledgment messages will be sent out to the HIH:

1. Validate the syntaxes;
2. Validate Semantics with the esMD affinity domain values;
3. Validate Payload Size;
4. Validate duplicate Unique ID for the message;
5. Validate participation of intended recipient claim reviewers;
6. Validate HIH OID authorization based on the CMS Onboarding; and
7. Cross validate RC OID and Content Type Code to check whether a particular RC accepts a document submission (e.g., PMD PAR, Responses to ADR, First Level Appeal Requests and Second Level Appeal Requests., ADMC, RA Discussion Requests, Non-Emergent Ambulance Transport PA Requests, or Hyperbaric Oxygen PA Requests).

This acknowledgment will be sent anywhere from less than one minute up to ten minutes after validation and is based on the size of attachment.

8.2.1.1 Success Message Without Warnings

```
<?xml version='1.0' encoding='UTF-8'?>
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    <To
      xmlns="http://www.w3.org/2005/08/addressing">http://localhost:8080/CONNECTAdapter/Adapte
      rComponentXDRResponse_Service</To>
    <Action
      xmlns="http://www.w3.org/2005/08/addressing">urn:gov:hhs:fha:nhinc:adaptercomponentxdres
      ponse:XDRResponseInputMessage</Action>
    <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
      <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
    </ReplyTo>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">5a3d7012-029e-4559-9a55-
    49e3d80d0190</MessageID>
  </S:Header>
  <S:Body>
    <ns21:AdapterRegistryResponse
      xmlns:ns2="http://schemas.xmlsoap.org/ws/2004/08/addressing"
      xmlns:ns3="http://www.w3.org/2005/08/addressing"
      xmlns:ns4="http://docs.oasis-open.org/wsn/b-2"
```

```

xmlns:ns5="http://docs.oasis-open.org/wsrf/bf-2"
xmlns:ns6="http://docs.oasis-open.org/wsn/t-1"
xmlns:ns7="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:ns8="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:ns9="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
xmlns:ns10="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
xmlns:ns11="http://www.hhs.gov/healthit/nhin"
xmlns:ns12="urn:ihe:iti:xds-b:2007"
xmlns:ns13="http://nhinc.services.com/schema/auditmessage"
xmlns:ns14="http://www.hhs.gov/healthit/nhin/cdc"
xmlns:ns15="urn:gov:hhs:fha:nhinc:common:subscriptionb2overrideforcdc"
xmlns:ns16="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:ns17="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ns18="urn:oasis:names:tc:emergency:EDXL:DE:1.0"
xmlns:ns19="urn:gov:hhs:fha:nhinc:common:subscriptionb2overridefordocuments"
xmlns:ns20="urn:gov:hhs:fha:nhinc:common:nhincommon"
xmlns:ns21="urn:gov:hhs:fha:nhinc:common:nhincommonadapter">
<ns21:assertion>
  <ns20:haveSecondWitnessSignature>>false</ns20:haveSecondWitnessSignature>
  <ns20:haveSignature>>false</ns20:haveSignature>
  <ns20:haveWitnessSignature>>false</ns20:haveWitnessSignature>
  <ns20:homeCommunity>
    <ns20:homeCommunityId>123.456.657.123</ns20:homeCommunityId>
  </ns20:homeCommunity>
  <ns20:userInfo>
    <ns20:personName>
      <ns20:familyName>na</ns20:familyName>
      <ns20:givenName>CMS</ns20:givenName>
      <ns20:secondNameOrInitials>Given Name - na C CMS Family Name -
</ns20:secondNameOrInitials>
      <ns20:fullName>CMS Given Name - na C CMS Family Name - na</ns20:fullName>
    </ns20:personName>
    <ns20:userName>abcd</ns20:userName>
    <ns20:org>
      <ns20:homeCommunityId>123.456.657.123</ns20:homeCommunityId>
      <ns20:name>QSSI the esMD Local Dev Gateway</ns20:name></ns20:org>
      <ns20:roleCoded><ns20:code>2.16.840.1.113883.6.96</ns20:code>
      <ns20:codeSystem>2.16.840.1.113883.6.96</ns20:codeSystem>
      <ns20:codeSystemName>SNOMED_CT</ns20:codeSystemName>
      <ns20:displayName>Claim Processing</ns20:displayName>
    </ns20:roleCoded>
  </ns20:userInfo>
  <ns20:authorized>>false</ns20:authorized>
  <ns20:purposeOfDisclosureCoded>

```



```

    </ns20:keyInfo>
    <ns20:signatureValue></ns20:signatureValue>
  </ns20:samlSignature>
  <ns20:messageId>5a3d7012-029e-4559-9a55-49e3d80d0190</ns20:messageId>
</ns21:assertion>
  <ns21:RegistryResponse requestId="esMD - Delivery To EnterpriseFileTransfer"
status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
    <ns7:ResponseSlotList>
      <ns8:Slot name="TransactionId">
        <ns8:ValueList>
          <ns8:Value>532</ns8:Value>
        </ns8:ValueList></ns8:Slot>
      <ns8:Slot name="ClaimId">
        <ns8:ValueList>
          <ns8:Value>69777777</ns8:Value>
        </ns8:ValueList></ns8:Slot>
      <ns8:Slot name="CaseId">
        <ns8:ValueList>
          <ns8:Value>6000045</ns8:Value>
        </ns8:ValueList>
      </ns8:Slot>
      <ns8:Slot name="contentTypeCode">
        <ns8:ValueList>
          <ns8:Value>1</ns8:Value>
        </ns8:ValueList>
      </ns8:Slot>
    </ns7:ResponseSlotList>
  </ns21:RegistryResponse>
</ns21:AdapterRegistryResponse>
</S:Body>
</S:Envelope>

```

8.2.1.2 Metadata Validation Errors

Table 19: Sample Error Message Content gives the sample first notification response “error message content” that will be sent for different scenarios.

The error messages listed in Table 19: Sample Error Message Content shall be sent in the First Notification Response.

Table 19: Sample Error Message Content

No.	Use Case	Scenario	First Notification Error Message
1.	All	Combination of Content Type Code, Healthcare FacilityType Code, Format Code and Class Code is incorrect	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_315 - The combination of the ContentType code, HealthcareFacilityType code, Format code and Class code is incorrect for this type of document submission. Please check the values of the codes and resubmit."/> </ns10:RegistryErrorList> </pre>
2.	All	Invalid Content Type Code	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_316 - The ContentType code is incorrect. The submission is not accepted. "/> </ns10:RegistryErrorList> </pre>
3.	All	Duplicate Submission	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSDuplicateUniqueIdInRegistry" codeContext=" THE ESMD_302 - Duplicate Claim document submission found, the Claim document submission was not accepted."/> </ns10:RegistryErrorList> </pre>
4.	All	NPI is incorrect	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_312 - Either NPI length or data type is incorrect; the submission is not accepted."/> </ns10:RegistryErrorList> </ns20:RegistryResponse> </pre>

No.	Use Case	Scenario	First Notification Error Message
5.	ADR and RA Discussion Requests	Claim ID format is incorrect	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_318 - The Claim ID was sent in the incorrect composite format. The correct format needs to be 'Claim ID ^^^&RCOID&ISO'. Please check the format and resubmit again." /> </ns10:RegistryErrorList> </pre>
6.	ADR and RA Discussion Requests	Case Id format is incorrect	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_319 - The Case ID was sent in the incorrect composite format. The correct format needs to be 'CaseID ^^^&RCOID&ISO'. Please check the format and resubmit again." /> </ns10:RegistryErrorList> </pre>
7.	ADR, ADMC Requests and RA Discussion Requests	Case Id is more than 32 characters in length	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_311 - Case ID is more than 32 characters; the submission is not accepted." /> </ns10:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
8.	Prior Authorization Requests (Power Mobility Device; Non-Emergent Ambulance Transport; HBO; and DMEPOS) and Pre-Claim Review (PCR) Demonstrations for HPCR Services requests.	Submission request contains Claim and Case Id tags	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_322 – Case ID is an invalid field for PA Requests."/> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_321 – Claim ID is an invalid field for PA Requests." /> </ns10:RegistryErrorList> </pre>
9.	All	Review Contractor does not accept a document submission	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode=" XDSRegistryMetadataErrorXDSHOIDIdDoesNotMatch" codeContext=" THE ESMD_317 - The Review Contractor to whom this submission was sent does not accept this particular document, identified by the ContentType code. Please change either the Review Contractor OID or the ContentType Code and submit again." /> </ns10:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
10.	ADR, (if included), and RA Discussion Requests	Claim Id for ADR, First Level Appeal Requests and Second Level Appeal Requests., and RA Discussions does not match either the 13 numeric or 15 numeric or 17-23 varchar	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_320 - Either the length or type of the Claim ID is incorrect. The Claim ID needs to be either 13 numeric or 14 numeric or 15 numeric or 17-23 varchar. Please check the format or length and resubmit again." /> </ns10:RegistryErrorList> </pre>
11.	ADR	For submissions to PERM Review Contractor a value for the esMDClaimId was sent or the PERM ID value which was sent in the esMDCaseld tag is not 11 alphanumeric characters	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_323 - For submissions to PERM, the esMDClaimId value needs to be blank and the esMDCaseld value needs to be the PERM Id which is 11 alphanumeric characters long. Please check the values and submit again." /> </ns10:RegistryErrorList> </pre>
12.	All	XDR submission request sent by the HIH could not be processed by the esMD Gateway because of system issues	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_000 - There was an error processing your request at this time by the esMD Data Application. Please retry. If you get the same error, please notify the esMD Help Desk." /> </ns10:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
12. Cont 1	No additional information	No additional information	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_203 - There was an error validating the HIH/RC OID because of system issues. Please retry. If you get the same error, please notify the esMD Help Desk." /> </ns10:RegistryErrorList> </pre>
12. Cont 2	No additional information	No additional information	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_313- There was an error validating the submission metadata because of system issues. Please retry. If you get the same error, please notify the esMD Help Desk." /> </ns10:RegistryErrorList> </pre>
13.	All	XDR submission request sent by the HIH gateway cannot be processed by the esMD Gateway since the payload size is more than 200 MB in size.	<pre> <ns3:RegistryErrorList> <ns3:RegistryError errorCode="XDSRegistryOutOfResources" codeContext=" THE ESMD_324 - The submission is not accepted because the esMD Gateway cannot process requests with a payload size more than 200 MB in size. Please make sure the encoded payload is less than 200 MB in size and resubmit." /> </ns3:RegistryErrorList> </pre>
14.	All	Copy files in Storage Area Network /Storage Area Network area is not available	<pre> <ns3:RegistryErrorList highestSeverity="ERROR"> <ns3:RegistryError severity="ERROR" errorCode="XDSRegistryOutOfResources" codeContext=" THE ESMD_001 - THE ESMD internal system error Please resubmit." /> </ns3:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
15.	All	File fails to copy to file transfer folder	<pre> <ns3:RegistryErrorList highestSeverity="ERROR"> <ns3:RegistryError severity="ERROR" errorCode="XDSRegistryOutOfResources" codeContext=" THE ESMD_002 - THE ESMD internal system error (File copy error). Please resubmit." /> </ns3:RegistryErrorList> </pre>
16.	All	File contains virus	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="CMSDocumentVirusScanError " codeContext=" THE ESMD_127 - THE ESMD validation error: Submission is infected with virus xxx." /> </ns10:RegistryErrorList> </pre>
17.	All	If file fails to decode	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSNonIdenticalHash" codeContext=" THE ESMD_128 - THE ESMD Processing error (Unable to decode submission). Please resubmit." /> </ns10:RegistryErrorList> </pre>
18.	All	File fails to zip	<pre> <ns3:RegistryErrorList highestSeverity="ERROR"> <ns3:RegistryError severity="ERROR" errorCode="XDSRegistryOutOfResources" codeContext=" THE ESMD_400 - THE ESMD internal system error (Compression error). Please resubmit." /> </ns3:RegistryErrorList> </pre>
19.	All	Payload is missing	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSMissingDocument" codeContext=" THE ESMD_369 - Submission is missing the payload. Please resubmit." /> </ns10:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
20.	All	Document ID inside metadata does not match the document ID assigned to payload	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryMetadataError" codeContext=" THE ESMD_368 - validation error: Document ID inside metadata does not match the Payload Document ID." /> </ns10:RegistryErrorList> </pre>
21.	All	MIME type is not correct	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSMissingDocumentMetadata" codeContext=" THE ESMD_367 - validation error: MIME type is not correct." /> </ns10:RegistryErrorList> </pre>
22.	All	Unzip file fails	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryError" codeContext=" THE ESMD_405 - Review Contractor Client processing error (Unzip failure). Please resubmit." /> </ns10:RegistryErrorList> </pre>
23.	All	Checksum does not match	<pre> <ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryError" codeContext=" THE ESMD_406 - Review Contractor Client processing error (Checksum issue). Please resubmit." /> </ns10:RegistryErrorList> </pre>

No.	Use Case	Scenario	First Notification Error Message
24.	XDR supporting documentation with CTC 13 for the previously submitted X12N 278 PA requests.	ACN does not match the ACN in the X12	<pre><ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryError" codeContext=" THE ESMD_376 - Attachment Control Number does not match the Attachment Control Number received in X12N 278 request. Provide matching X12N 278 Attachment Control Number and resubmit." /> </ns10:RegistryErrorList></pre>
25.	XDR supporting documentation with CTC 13 for the previously submitted X12N 278 PA requests.	Invalid ACN	<pre><ns10:RegistryErrorList highestSeverity="ERROR"> <ns10:RegistryError severity="ERROR" errorCode="XDSRegistryError" codeContext=" THE ESMD_377 - Incorrect format/length of the Attachment Control Number. Provide a valid X12N 278 Attachment Control Number and resubmit." /> </ns10:RegistryErrorList></pre>

8.3 The esMD System Second Notification

8.3.1 Claim Review Pickup Status Notification

A Notification message will be sent to the HIH after the RC picks up the submitted documents from the TIBCO MFT Server. This time to receive this notification acknowledgment is dependent upon the RC inbound submission pulling process from the TIBCO MFT Server. If no response is received after eight hours, the sender should contact the esMD Support team (esMD_Support@cms.hhs.gov).

```
<ns2:RegistryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
  xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-
  regrep:xsd:query:3.0" xmlns:ns4="http://www.hhs.gov/healthit/nhin"
  xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0" requestId="esMD - Review Contractor
  Pick up the documents from CMS Enterprise File Transfer" status="urn:oasis:names:tc:ebxml-
  regrep:ResponseStatusType:Success">
```

```
<ns2:ResponseSlotList>
  <Slot name="esMDTransactionId">
    <ValueList>
      <Value>1076795</Value>
    </ValueList>
  </Slot>
  <Slot name="esMDClaimId">
```

```
<ValueList>
  <Value>Claim5678901234568</Value>
</ValueList>
</Slot>
<Slot name="esMDCaseld">
  <ValueList>
    <Value>AA90133333301</Value>
  </ValueList>
</Slot>
<Slot name="contentTypeCode">
  <ValueList>
    <Value>1</Value>
  </ValueList>
</Slot>
<Slot name="HIHTo THE ESMDDeliveryTimeStamp">
  <ValueList>
    <Value>20150212112455</Value>
  </ValueList>
</Slot>
<Slot name=" THE ESMDClaimReviewerPickUpTimeStamp">
  <ValueList>
    <Value>20150212112455</Value>
  </ValueList>
</Slot>
<Slot name=" THE ESMDPickedUpClaimReviewer">
  <ValueList>
    <Value>urn:oid:2.16.840.1.113883.13.34.110.1.999.2</Value>
  </ValueList>
</Slot>
</ns2:ResponseSlotList>
</ns2:RegistryResponse>
```

8.3.2 Claim Review Pickup Error Notification

This notification message is sent to HIH in the event there is an error in processing the downloaded file at RC end or in the TIBCO MFT Server. If no response is received after eight hours, the sender should contact the esMD Support team (esMD_Support@cms.hhs.gov).

```
<ns2:RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure"
  requestId="esMD - Review Contractor Pickup the documents from CMS Enterprise File
  Transfer">
```

```
<ns4:ResponseSlotList>
```

```
<ns3:Slot name="esMDTransactionId">
```

```
<ns3:ValueList>
```

```
<ns3:Value>996</ns3:Value>
```

```
</ns3:ValueList>
```

```
</ns3:Slot>
```

```
<ns3:Slot name="HIHTo THE ESMDDeliveryTimeStamp">
```

```
<ns3:ValueList>
```

```
<ns3:Value>20150211121249</ns3:Value>
```

```
</ns3:ValueList>
```

```
</ns3:Slot>
```

```
<ns3:Slot name=" THE ESMDClaimReviewerPickUpTimeStamp">
```

```
<ns3:ValueList>
```

```
<ns3:Value>20150211121249</ns3:Value>
```

```
</ns3:ValueList>
```

```
</ns3:Slot>
```

```
<ns3:Slot name=" THE ESMDPickedUpClaimReviewer">
```

```
<ns3:ValueList/>
```

```
</ns3:Slot>
```

```
</ns4:ResponseSlotList>
```

```
<ns4:RegistryErrorList highestSeverity="urn:oasis:names:tc:ebxml-
regrep:ErrorSeverityType:Error">
```

```
<ns4:RegistryError codeContext="Review Contractor Client processing error (Unzip failure).
Please resubmit"
```

```
  errorCode="XDSRegistryMetadataError"
```

```
        severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"/>  
</ns4:RegistryErrorList>  
</ns2:RegistryResponse>
```

8.4 The esMD System Third Notification

8.4.1 PA Review Response

This notification message includes PA Review Response in the event RC has determined their decision for a PA request. The notification message could include 3 types of responses i.e.

- Affirmed (A) - An Affirmed response denotes that the RC has successfully approved the PA request. See Section 10.8.1, Affirmed PA Review Results Response for more details.
- Non-Affirmed (N) - A Non-Affirmed response denotes that the RC has not approved the PA request for one or more reasons. See Section 10.8.2, Non-Affirmed PA Review Results Response for more details.
- Affirmed with a Change (M) - A Affirmed with a Change response denotes that the RC has partly approved the PA request for one or more reasons. See Section 10.8.3, Modified PA Review Results Response for more details.

CMS mandates that the Review Contractor submit a response for a PA request received by the Review Contractor within ten business days. If neither a PA review response nor a PA review error response is received after ten days, the sender should contact the esMD Support team (esMD_Support@cms.hhs.gov).

8.4.2 PA Review Error Response

This notification message includes PA Error Response in the event RC has determined their decision for a PA request. The notification message includes a Reject (R) response from RCs. A Rejected response denotes that the RC has completely rejected the PA request for one or more reasons.

If no response is received after ten days, the sender should contact the esMD Support team (esMD_Support@cms.hhs.gov).

See Section 10.8.4 Rejected PA Review Results Response for more details.

8.4.3 Review Contractor Administrative Error Notification

This notification message includes an Administrative Error Response in the event RC encounters issues on inbound submissions. The notification message could include 4 types of responses i.e.

- Corrupt Files/Cannot Read Files;
- Submission Send to Incorrect RC;
- Virus Found; and
- Other.

These Administrative Error Responses are sent to respective HIH as well as the esMD Support team to resolve manually. A sample Administrative Error Response XML message is shown below:

```
<ns17:RegistryResponse requestId="esMD – Administrative Error Notification"
  status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
  <ns6:ResponseSlotList>
    <ns5:Slot name="esMDTransactionId">
      <ns5:ValueList>
        <ns5:Value>12812678</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
  </ns6:ResponseSlotList>
  <ns6:RegistryErrorList highestSeverity="ERROR">
    <ns6:RegistryError severity="ERROR"
      errorCode="RCAdministrativeError"
      codeContext=" THE ESMD_410 - Files that were received by Review Contractor have been
corrupt."/>
    <ns6:RegistryError severity="ERROR"
      errorCode="RCAdministrativeError"
      codeContext=" THE ESMD_411 - The Submission is sent to incorrect Review Contractor."/>
    <ns6:RegistryError severity="ERROR"
      errorCode="RCAdministrativeError"
      codeContext=" THE ESMD_412 - Files that were received by Review Contractor have been
infected with virus."/>
    <ns6:RegistryError severity="ERROR"
      errorCode="RCAdministrativeError"
      codeContext=" THE ESMD_413 - Review Contractor cannot read the files that have been
submitted."/>
    <ns6:RegistryError severity="ERROR"
      errorCode="RCAdministrativeError"
      codeContext=" THE ESMD_414 - Other errors encountered by Review Contractor."/>
  </ns6:RegistryErrorList>
</ns17:RegistryResponse>
```

8.5 Information Contained in Response Message

HIHs should look for the following information in the response message: Message ID, Unique ID, Request ID, Status, and Response Slots.

8.5.1 Message ID (Correlated with Request MessageID)

To correlate the Request MessageID with the response message, the message ID will be copied back to the response message.

Example:

```
<S:Header>
.....
<MessageID xmlns="http://www.w3.org/2005/08/addressing">5a3d7012-029e-4559-9a55-49e3d80d0190</MessageID>
</S:Header>
```

8.5.2 Unique ID (Correlated with Request UniqueID)

To correlate the request UniqueID with the response, the Request UniqueID will be copied back to response message under Assertion.ID.

Example:

```
<ns20:assertion>
<ns20:id>40df7c0a-ff3e-4b26-baeb-f2910f6d0mc202</ns20:id>
```

8.5.3 RequestID

The RequestID explains the type of response Type. Table 20: Possible Request Types lists the possible request types:

Table 20: Possible Request Types

No.	Request Type String	Request Type in Response Messages
1.	The esMD - HIH and RC OID Authorization The esMD - RC OID and ContentType Code Cross Validation	First Notification Response
2.	The esMD - Document Submission Generic Validation	First Notification Response
3.	The esMD - Meta Data Validation and Persistence	First Notification Response
4.	The esMD - Delivery To CMS Enterprise File Transfer System	First Notification Response

No.	Request Type String	Request Type in Response Messages
5.	The esMD - RC picks up the documents from the CMS Enterprise File Transfer system	Second Notification Response
6.	The esMD – Payload Virus Scan	Third Notification Response

Example:

```
<ns21:RegistryResponse requestId="esMD - Delivery To EFT" status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
```

8.5.4 Status

Status describes the status of the message:

1. urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success;
2. urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Warning; or
3. urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Error.

Example:

```
<ns2:RegistryResponse xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0" xmlns:ns4="http://www.hhs.gov/healthit/nhin"
xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0" requestId="esMD - Delivery To CMS
Enterprise File Transfer" status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
```

```
<ns2:ResponseSlotList>
  <Slot name="esMDTransactionId">
    <ValueList>
      <Value>1076201</Value>
    </ValueList>
  </Slot>
  <Slot name="esMDClaimId">
    <ValueList>
      <Value>Claim5678901234568</Value>
    </ValueList>
  </Slot>
  <Slot name="esMDCasId">
```

```

<ValueList>
  <Value>AA9013333301</Value>
</ValueList>
</Slot>
<Slot name="contentTypeCode">
  <ValueList>
    <Value>1</Value>
  </ValueList>
</Slot>
</ns2:ResponseSlotList>
</ns2:RegistryResponse>

```

Note: In addition to the statuses listed above, the esMD also uses:

urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure.

In the future, both Error and Failure strings will be merged and only the ‘Error’ string shall be used.

8.5.5 Response Slots

The esMD specific response slots will have the esMD transaction information. The information in the slots is related to the following:

1. TransactionId;
2. CaseId;
3. ClaimId; and
4. contentType Code.

Example:

```

<ns7:ResponseSlotList>
  <ns8:Slot name="TransactionId">
    <ns8:ValueList>
      <ns8:Value>532</ns8:Value>
    </ns8:ValueList></ns8:Slot>
  <ns8:Slot name="ClaimId">
    <ns8:ValueList>
      <ns8:Value>69777777</ns8:Value>
    </ns8:ValueList></ns8:Slot>
  <ns8:Slot name="CaseId">
    <ns8:ValueList>
      <ns8:Value>6000045</ns8:Value>
    </ns8:ValueList>
  </ns8:Slot>

```

```
<ns8:Slot name="contentTypeCode">  
  <ns8:ValueList>  
    <ns8:Value>1</ns8:Value>  
  </ns8:ValueList>  
</ns8:Slot>  
</ns7:ResponseSlotList>
```

8.5.6 Delivery to the CMS Enterprise File Transfer System (First Notification)

In the event the sender does not receive the first notification response within 20 minutes of the document submission, the sender may take the following steps.

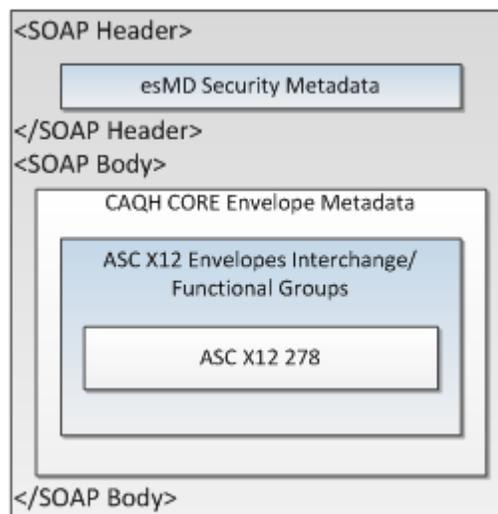
1. The sender can resubmit the claim documentation a second time. After this second submission, the sender should allow 20 minutes to receive an acknowledgement response.
2. The sender may attempt submissions for a total of three attempts. If the acknowledgement is not received after the third attempt, the sender should contact the esMD Support team (esMD_Support@cms.hhs.gov) for further resolution.

9 The esMD System CAQH Profile

9.1 Request Layout

The esMD implemented the Healthway (previously the Nationwide Health Information Network (NHIN)) Phase II CAQH CORE Rule 270: Connectivity Rule Version 2.2.0 to exchange ASC X12 Administrative Transactions with HIHs via the Internet. CONNECT support for CAQH Profile has been implemented as part of the CONNECT release 4.4. The “CAQH CORE X12 Document Submission Service Interface Specification” defines specific constraints on the use of the CAQH CORE Connectivity Rule. Figure 5: ASC X12N 278 5010 over CONNECT (CAQH CORE 270) presents the components of a request or response message using 278 and CONNECT with the NHIN CAQH CORE X12 Document Submission Service Interface Specification.

Figure 5: ASC X12N 278 5010 over CONNECT (CAQH CORE 270)



9.2 CAQH CORE Real-Time Mode (Synchronous) and CAQH CORE Generic Batch Mode (Deferred) Messaging

HIHs planning to submit X12N 278 5010 requests to the esMD system must implement the Phase II CAQH CORE Rule 270 Connectivity Rule, Version 2.2.0.

This connectivity rule allows for the following two modes of messaging:

- Real time mode (i.e. Synchronous); and
- Batch mode (i.e. Deferred).

The HIH shall use the real time mode, i.e. synchronous messaging, for sending an X12N 278 5010 request to the esMD system. In this real time mode, the HIH that sent the X12N 278 5010 request shall receive a response for that request within 20 seconds. This response is considered to be the equivalent of the "first notification" used in the XDR profile.

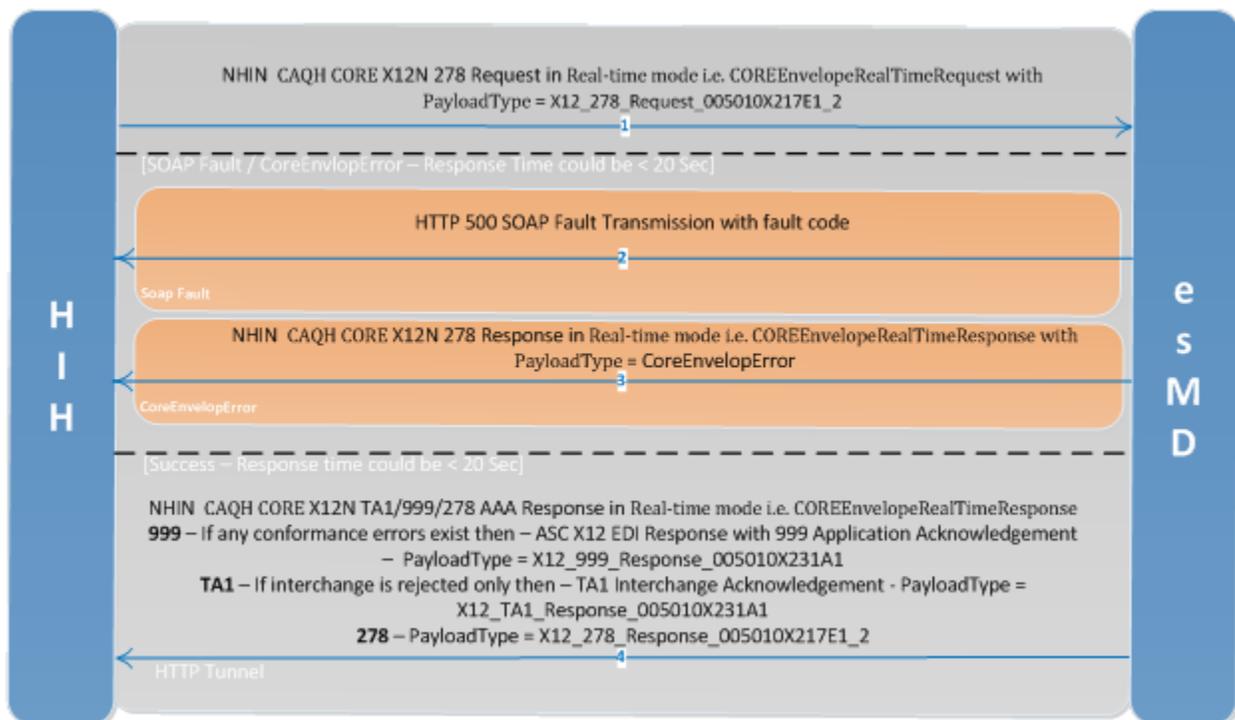
The esMD system shall send the "second notification", i.e. the "pickup status/error" notification and the "third notification", i.e. the "PA Review Response", using the Batch mode (i.e. for deferred messaging).

The difference between the real time and the batch mode, other than the response times, is that the Message Transmission Optimization Mechanism (MTOM) is used for sending an attachment in the batch mode.

9.3 HIH to the esMD - CAQH PA Request (Real Time)

1. HIH submits to the esMD a X12N 278 5010 real-time authorization request in CAQH envelope. Appendix I The esMD Sample CAQH Real-Time Request shows an example of a CAQH real-time request.

Figure 6: X12 PA Request in CAQH Real Mode



- Once the esMD has identified the request as a X12N 278 5010, the esMD will have a fixed amount of time to process the request. (20 seconds for real-time) Otherwise, the request times out. If the request times out, the HIH will get a timeout error and will need to resubmit the request.
2. If the esMD is unavailable, the HIH will receive a HTTP 500 error.
 3. If there are any Errors in the CAQH envelope, the HIH will receive a COREEnvelopeRealTimeResponse with PayloadType as CoreEnvelopError
 4. The esMD will process the CAQH request and retrieve the EDI payload. A response is created the same business day (within 20 seconds) the file is submitted and sent back to the HIH.

- If data in the ISA segment is not valid and the EDI payload could not be extracted, the esMD will send a COREEnvelopeRealTimeResponse with PayloadType as CoreEnvelopError and appropriate error message.
- If the interchange is rejected, A TA1 Interchange Acknowledgement is generated and sent back to the HIH. Please refer to the companion guide in the section below (link to the relevant section here) for more details.
- A real-time acknowledgement is created and sent back to the HIH if the submitted the X12N 278 5010 file fails format edits.
 - i. If there are any conformance errors, a 999 error response is generated, unless a TA1 rejection occurred. Please refer to the companion guide in the section below (link to the relevant section here) for more details.
- Transactions that pass the validation process, but fail further in the processing (for example; ineligible member) will generate a 278 real-time response, to include an AAA segment indicating the nature of the error. Please refer to the companion guide in the section below (link to the relevant section here) for more details.

9.3.1 Traceability Between Requests and Responses

The X12 278 5010 provides several methods of tracing documents between requesters and matching them to responses to the original requests. Refer to the ASC X12N 278 5010 (005010X217) Implementation guide at <http://store.x12.org/store/healthcare-5010-original-guides>, Section 1.11.4 for additional documentation on the usage of these methods to trace and match requests with responses. Traceability is important in both paper-based exchanges and electronic exchanges of documents. Matching responses to their original requests should be accommodated through the available X12 data segments, which should appear in metadata or paper cover sheets (e.g., fax transmissions). There are three primary methods of providing traceability in the X12 278 5010:

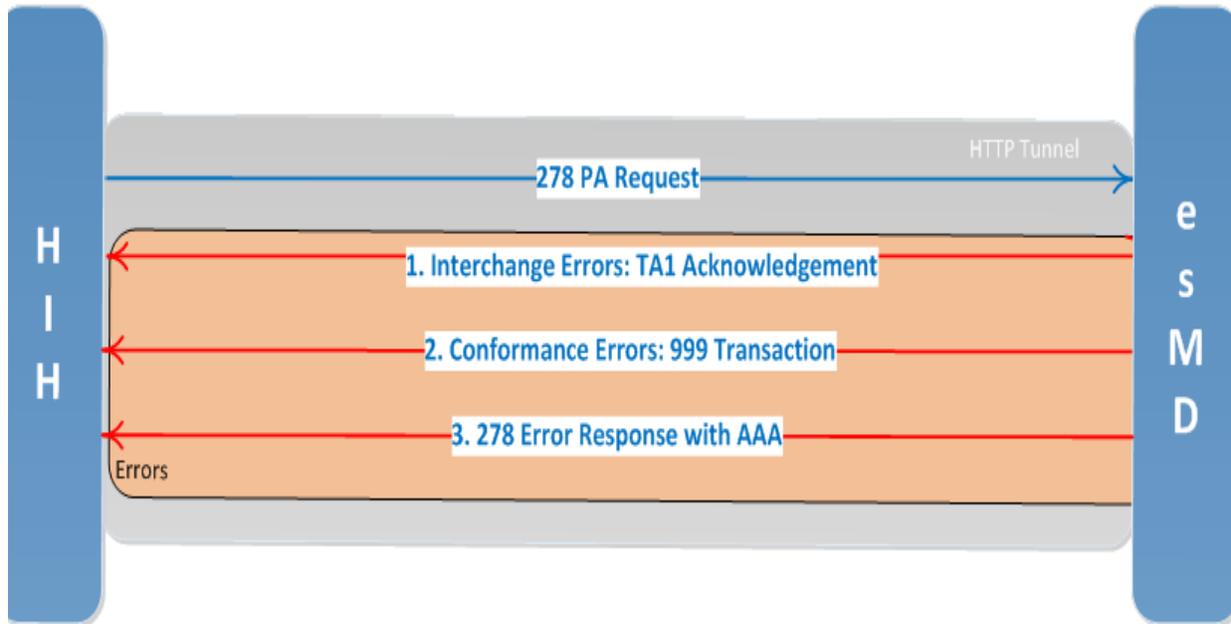
- The BHT03 element (*Reference Identification*, also known as *Submitter Transaction Identifier*) must be returned in a response 278 (in the same BHT03 element). This data element provides traceability at the transaction level (as opposed to the event/service level, as seen below).
- The TRN segment appears in both the 2000E loop (*Patient Event*) where it serves as the Patient Event Tracking Number and it can appear in the 2000F loop (*Service*) as the Service Trace Number.
- The PWK06 element (Identification Code, also known as the Attachment Control Number) within the 2000E and 2000F loops is required when responding to requests for electronic data when using another ASC X12N standard (e.g., the ASC X12N 275 (006020X278) or LOINC codes as used in the HI segment of the 278). When using the ASC X12N 275 transaction set to support the sending of documentation in response to a 278, the required TRN02 element (Attachment Control Trace Number)—found in loop 2000A of the 275 guide—will be populated with the PWK06 code found in the 278.

Note: Please refer to the Section 5.3.39 Attachment Control Number (ACN) for more details on how the ACN is used to link the X12N 278 5010 request and the XDR supporting documentation request.

9.3.2 X12N 278 5010 Acknowledgements

For a summary of X12 transaction errors and acknowledgments for the 278, refer to Figure 7: X12N 278 5010 Acknowledgements.

Figure 7: X12N 278 5010 Acknowledgements



Because transactions in this guide are limited to exchange of the ASC X12N 278 5010, transaction-level error handling occurs, as defined by the relevant ASC X12 standards.

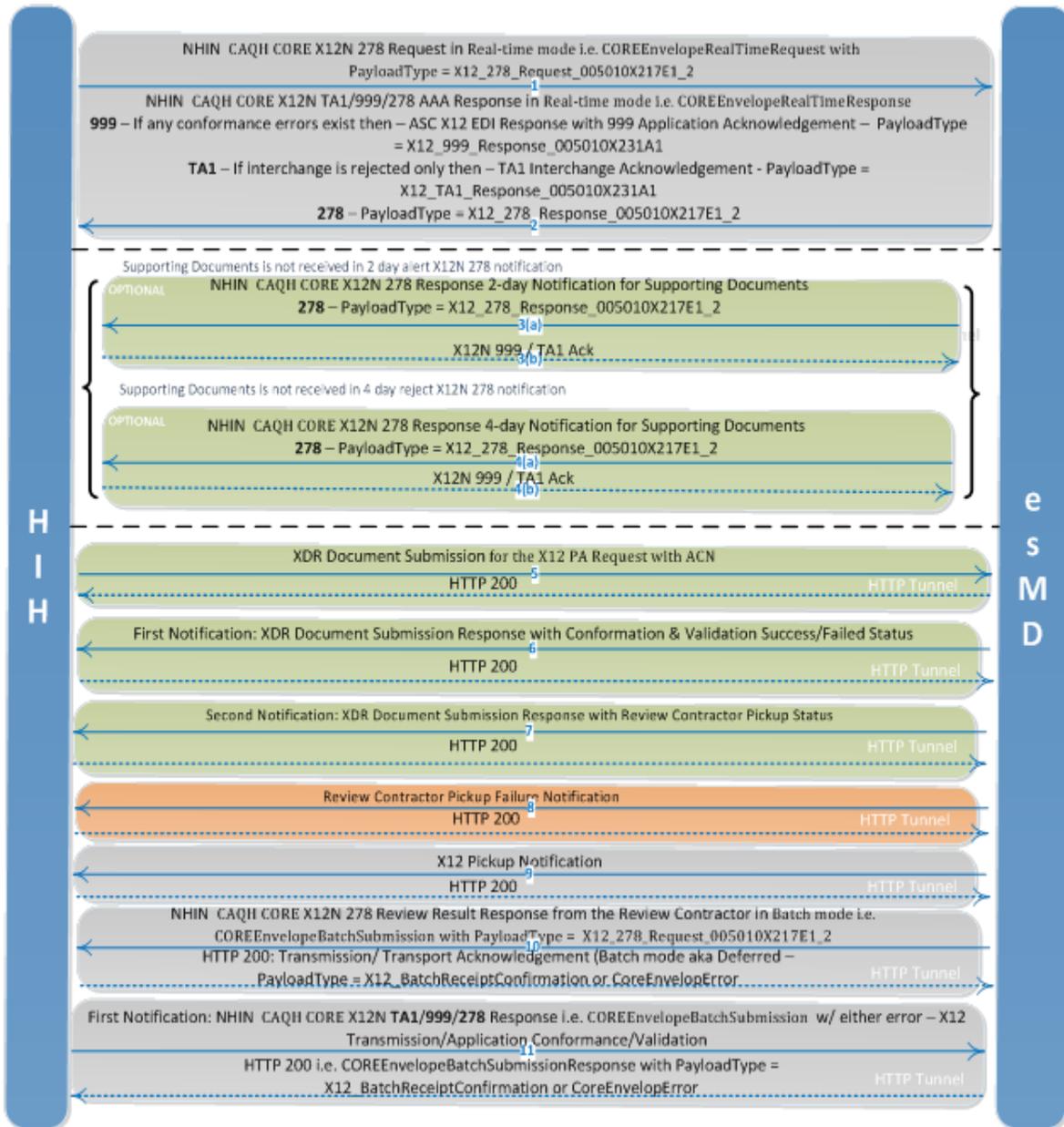
1. ASC X12 Interchange Envelope Conformance errors in the esMD ASC X12N 278 5010 transaction shall be communicated in an ASC X12 TA1 response. The possible TA1 error codes are located in the ASC X12 TA1 005010X231A1 Implementation Specification.
2. ASC X12 Standard Conformance & Implementation Guide Conformance errors in the esMD ASC X12N 278 5010 transaction shall be communicated in an ASC X12 999 response. The possible 999 error codes are located in the ASC X12 999 005010X231A1 Implementation Specification.

Please refer to the companion guide that is available at <http://store.x12.org/store/healthcare-5010-original-guides> for more details. The relevant ASC X12 Implementation Guides for error and acknowledgment handling are also available at <http://store.x12.org/store/healthcare-5010-original-guides>.

9.4 The esMD X12N 278 5010 PA Request with XDR Additional Documentation

Figure 8: X12N 278 5010 PA Request with Additional XDR Documentation depicts the X12N 278 5010 Workflow with additional XDR document submission(s) and the PA Review Responses coming from RC to HIH.

Figure 8: X12N 278 5010 PA Request with Additional XDR Documentation



1. The HIH sends the X12N 278 5010 PA Request in CAQH format (i.e., COREEnvelopeRealTimeRequest with PayloadType = X12_278_Request_005010X217E1_2) to the esMD.
2. The esMD processes the PA request.
3. The esMD generates the appropriate response, as described in the Section 9.2 CAQH CORE Real-Time Mode (Synchronous) and CAQH CORE Generic Batch Mode (Deferred) Messaging.
4. HIHs planning to submit X12N 278 5010 requests to the esMD system must implement the Phase II CAQH CORE Rule 270 Connectivity Rule, Version 2.2.0.

This connectivity rule allows for the following two modes of messaging:

- Real time mode (i.e. Synchronous); and
- Batch mode (i.e. Deferred).

The HIH shall use the real time mode, i.e. synchronous messaging, for sending an X12N 278 5010 request to the esMD system. In this real time mode, the HIH that sent the X12N 278 5010 request shall receive a response for that request within 20 seconds. This response is considered to be the equivalent of the "first notification" used in the XDR profile.

The esMD system shall send the "second notification", i.e. the "pickup status/error" notification and the "third notification", i.e. the "PA Review Response", using the Batch mode (i.e. for deferred messaging).

The difference between the real time and the batch mode, other than the response times, is that the Message Transmission Optimization Mechanism (MTOM) is used for sending an attachment in the batch mode.

5. HIH sends the CAQH PA Request (in Real Time) to the esMD.
6. The esMD checks the PWK segment of the X12N 278 5010 EDI payload to see if it has acceptable values i.e., EL or FT.
7. The esMD checks the PWK06 element (Identification Code, also known as the Attachment Control Number) within the 2000E and 2000F loops.
8. If any of these fields fail validation, the request is rejected immediately.
9. The esMD waits for the additional documentation to be sent by the HIH in XDR Deferred Document Submission.
10. After two (2) business days have expired, an X12N 278 5010 response with a 'pending' status that requests documentation be sent immediately will be received by HIH. All PHI data will be masked in the response if the HIH does not sign the CMS esMD agreement. HIHs with a valid agreement will receive the PHI unmasked in the response.
 - A value of 19 in Segment "BHT" and Element Position 06 denotes "further updates to follow"; and
 - A value of A4 in Segment "HCR 03" denotes "Pended" for 2 business day notification.
11. The HIH responds to the 2 day notification with a X12N 999 success status or a 999 error/TA1 acknowledgement in case of error.

12. If the HIH has not responded to the 2 day notification with supporting documentation in XDR format, after four (4) business days after the initial X12N 278 5010 has been sent have expired:
 - a. The esMD sends a X12N 278 5010 rejection response to the HIH.
 - i. A value of 18 in Segment "BHT" and Element Position 06 denotes a "rejection" status. As with the pending response, all PHI data will be masked.
 - ii. A value of "C" in Segment "HCR 03" segment denotes "rejection".
 - b. The HIH responds with a X12N 999 success status or a 999 error/TA1 acknowledgement in case of error.
13. The HIH sends the additional documentation to the esMD in XDR Deferred Document Submission with the ACN that corresponds to the X12N 278 5010 PA Request sent earlier.
14. The esMD validates all the metadata in the XDR request as described in the section 6 XDR Validation and sends a response to the HIH as a first notification (see section 8.1.2 Error Messages).
15. The esMD packages the XDR additional documentation and the PA Request together and sends the package to the RC via MFT.
 - a. The RC pulls the PA request package using the RC Client.
 - b. The RC processes the PA request package in their downstream systems.
 - c. The esMD will send this RC pickup notification with error to the HIH.
16. If there are any errors in processing the PA request, the RC sends a pickup notification with the corresponding error to the esMD which will be forwarded to the HIH as a Review Contractor Pickup Failure Notification. The HIH will need to resubmit the PA request to the esMD.
17. The X12 Pickup Notification will be sent to HIH if the RC was successful in processing the package sent from the esMD.
18. The RC generates a PA Review Results Response and sends it to the esMD via MFT using the RC Client.
 - a. The esMD processes the PA Review Results Response received from the RC.
 - b. If there are any errors in the PA Review Results Response received from the RC, the esMD sends a validation error to the RC.
 - c. The RC corrects the errors and resubmits the PA Review Results Response.
 - d. The esMD generates the X12N 278 5010 PA response as described in Section 9.5, The esMD to HIH - CAQH PA Review Result Response (Batch Mode) and sends it to the HIH.
19. The HIH responds to the esMD with appropriate response for the PA Response received (see Section 9.5, The esMD to HIH - CAQH PA Review Result Response (Batch Mode)).

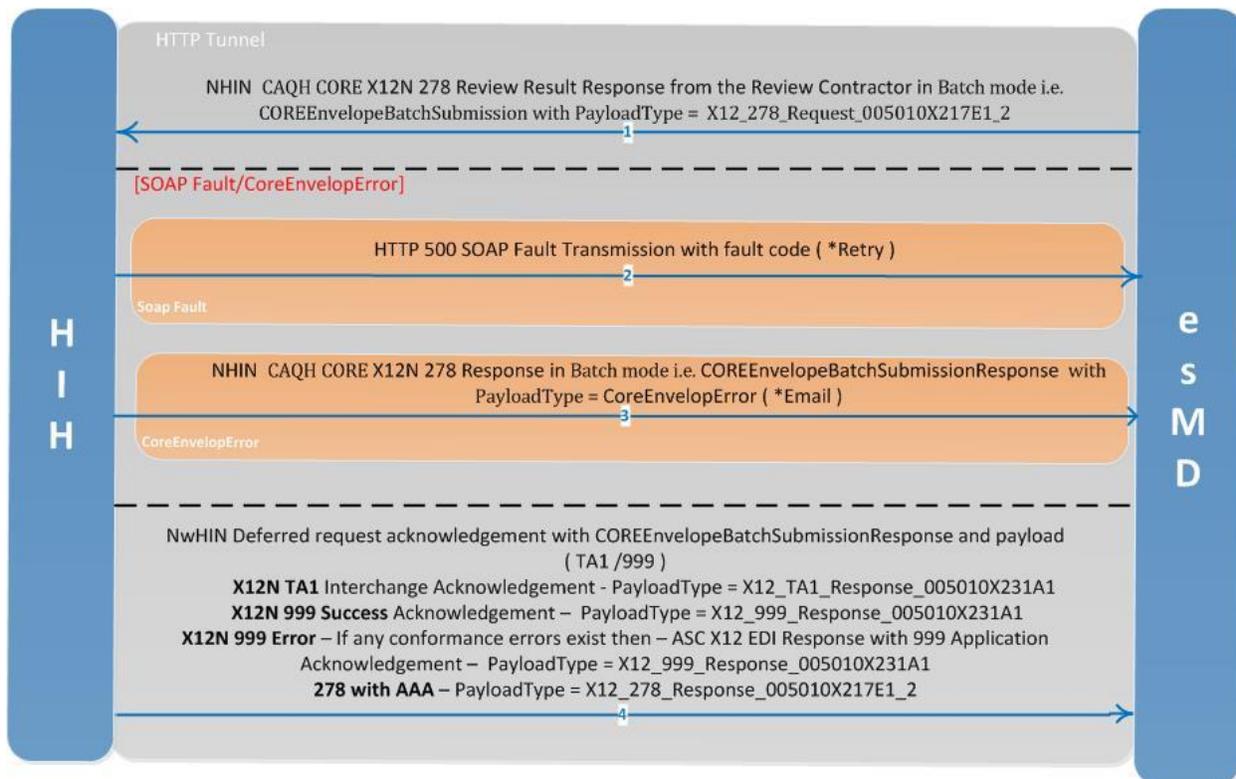
9.5 The esMD to HIH - CAQH PA Review Result Response (Batch Mode)

1. The PA Review Results Response from the Review Contractor is sent to the HIH by the esMD using the CAQH Batch mode transmissions. The CAQH Batch mode transmissions differ from the CAQH Real time transmissions in two ways:

- a. The response to the Batch mode transmission does not have to be synchronous or timed as in Real time transmission.
 - b. The payload is sent as an attachment using Message Transmission Optimization Mechanism (MTOM) in Batch mode transmissions where as in Real time transmissions, the payload is sent inline.
2. The Batch mode response can carry the following payload types:
- a. TA1 for interchange errors
 - b. 999 error in case of conformance errors.
 - c. 999 success in case of successful receipt.

Figure 9: X12 PA Review Result Response in CAQH Batch Mode illustrates the PA Review Result Response in CAQH Batch Mode.

Figure 9: X12 PA Review Result Response in CAQH Batch Mode



1. The esMD receives a PA Review Results Response from the RC.
 - The esMD will validate the PA Review Results Response and processes it.
 - The esMD will generate an X12N 278 5010 Response from the PA Review Result Response received from the RC.
 - The esMD sends the X12N 278 5010 Response to the HIH in the Phase II CAQH CORE Rule 270: Connectivity Rule Version 2.2.0 SOAP envelope over HTTP.

- The CAQH COREEnvelopeBatchSubmission with PayloadType X12_278_Request_005010X217E1_2 is used to send this X12N 278 5010 Response to the HIH.
2. If the HIH Gateway is unavailable or encountered an internal server error, the esMD will receive an HTTP 500 error.
 - The esMD Gateway will try to send the response once again as a new request.
 - If the second attempt fails, the esMD scheduler will try to send the PA Review Results Response again after 3 hours.
 - This round of retries is limited to 3 attempts again.
 - In case ALL three attempts fail, the esMD will let the Helpdesk know of this incident in order to communicate the failure to the HIH.
 3. If the HIH encounters an error processing the CAQH Batch Request sent from the esMD, the HIH will send a CoreEnvelopeError back to the esMD. The esMD will generate and send an email notification to the Helpdesk to inform the esMD contractor of this error. The helpdesk will contact the HIH to debug if there are any issues with processing the CAQH Batch requests.
 4. The HIH responds with a HTTP 200 i.e., COREEnvelopeBatchSubmissionResponse with PayloadType either X12_BatchReceiptConfirmation. The HIH generates the First Notification, i.e., COREEnvelopeBatchSubmission with one of the following and sends it to the esMD.
 - In the event of an error, i.e., X12 Transmission/Application Conformance/Validation Error:
 - TA1: If interchange is rejected only – TA1 Interchange Acknowledgement - PayloadType = X12_TA1_Response_005010X231A1
 - 999 Error: If any conformance errors exist then – ASC X12 EDI Response with 999 Application Acknowledgement – PayloadType = X12_999_Response_005010X231A1
 - If the HIH has successfully received the PA Review Response, the esMD will receive a 999 Success Acknowledgement with PayloadType = X12_999_Response_005010X231A1

9.6 CAQH Metadata

Phase II CAQH CORE Rule 270: Connectivity Rule Version 2.2.0 defines a set of metadata used for message routing, transaction auditing, transaction scheduling, resource allocation, backward compatibility, error handling, and audit logging. The required CAQH CORE Metadata for the esMD is listed in Table 21: CORE Envelope Metadata.

Table 21: CORE Envelope Metadata

CORE Field	Requirement	Data Type	Definition	Value or Field Constraints for the esMD 's eDoC
PayloadType	R	Coded Set	Payload Type specifies the type of payload included within the request/response, (e.g., HIPAA ASC X12 transaction set 278).	X12_278_Request_005010 X217E1_2 X12_278_Response_00501 0X217E1_2 CoreEnvelopeError X12_TA1_Response_00501 X231A1 X12_999_Response_00501 0X231A1
ProcessingMode	R	Coded Set	Processing Mode indicates Batch or Real-time processing mode (as defined by CORE)	RealTime/Batch
PayloadLength	R	Integer	Specifies the length of the actual payload in bytes.	Base 10
PayloadID	R	String	<p>Payload ID (unique within the domain of the party that sets this value) is a payload identifier assigned by the sender. If the payload is being resent in the absence of confirmation of receipt to persistent storage, the same PayloadID may be re-used.</p> <p>PayloadID will conform to ISO UUID standards (described at ftp://ftp.rfc-editor.org/in-notes/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address, to ensure uniqueness.</p>	Unique the esMD Message ID

CORE Field	Requirement	Data Type	Definition	Value or Field Constraints for the esMD 's eDoC
TimeStamp	R	dateTime	The Sender (request) or Receiver (response) Time Stamp combines time and date message metadata into a single Coordinated Universal Time (UTC) time stamp (including time zone information) specifying when a message is created and sent to a receiver. This does not require a shared time server for consistent time.	Date and Time the Message was created (http://www.w3.org/TR/xmlschema11-2/#dateTime)
SenderID	R	String	A unique business entity identifier representing the message envelope creator.	HIH OID
ReceiverID	R	String	A unique business entity identifier representing the next-hop receiver.	esMD OID
CORERuleVersion	R	Coded Set	The CORE Rule version that this envelope is using. This value can be used to maintain backward compatibility when parsing/processing messages.	v2.2.0
Checksum	R	String	An element used to allow receiving site to verify the integrity of the message that is sent.	Algorithm is SHA-1, Encoding is hexadecimal. Checksum must be computed only on the payload and not on the metadata.
ErrorCode	R (for a response to an ASC X12 transaction)	Coded Set	Error code to indicate the error when processing the envelope (includes "Success" response).	Refer to Phase II CAQH CORE Rule 270: Connectivity Rule Version 2.2.0 Section 4.3.3.2 for appropriate codes

CORE Field	Requirement	Data Type	Definition	Value or Field Constraints for the esMD 's eDoC
ErrorMessage	R (for a response to an ASC X12 transaction)	String	Text Error message that describes the condition that caused the error. The text of the ErrorMessage must provide additional information describing how the Error can be resolved, and must not provide conflicting information from that provided in the ErrorCode.	N/A

9.7 Error Handling

This section follows error handling specified in Section 4.3.3 of the Phase II CAQH CORE 270: Connectivity Rule Version 2.2.0. Envelope level errors shall be handled in accordance with Phase II CAQH CORE Rule 270: Connectivity Rule Version 2.2.0. “To handle CORE-compliant envelope processing status and error codes, two fields called errorCode and errorMessage are included in the CORE-compliant Envelope. The errorMessage is a free form text field that describes the error for the purpose of troubleshooting/logging. When an error occurs, PayloadType is set to “CoreEnvelopeError.”

9.8 CONNECT SAML Assertions

CONNECT SAML Assertions define the exchange of metadata used to characterize the initiator of a request. The purpose of this SAML Assertion exchange is to provide the esMD with the information needed to make an authorization decision using the policy enforcement point for the requested the esMD function. Each HIH initiating SOAP message must convey information regarding the sender’s attributes and authentication using SAML 2.0 Assertions. SAML assertions for the esMD eDoC must conform to the NHIN Authorization Framework Specification v3.0. SAML assertions for the esMD must conform to Section 5.3.6, SAML Assertions.

9.9 X12N 278 5010 Companion Guide

For details on the X12N 278 5010 requests and responses and the PHI Masking, refer the Companion Guide available here:

https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Information_for_HIHs.html

10 XDR PA Response

10.1 Overview

The esMD Gateway is accepting Prior Authorization Requests (PARs) from the HIHs as X12 and/or XDR submissions. The recipients of these requests are the RCs. These submission requests are identified based on the Content Type Code, which is a submission set metadata element in the XDR submission request sent by the HIHs.

The outbound responses from the RCs shall be called PA review results responses. It is important to note that the RCs shall be able to send outbound PA review results responses for XDR and X12 requests using the esMD for only those PARs, which were sent by the HIHs using inbound the esMD. In addition, using outbound the esMD, RCs shall be able to send only one valid outbound PA review results response for a PAR (i.e., one response per one request).

10.2 XDR PA Review Results Response

The PA review results responses sent by the RCs shall be structured, in XML format.

10.2.1 XDR Review Response Data Elements

The PA Review Results Response for XDR will be composed of the following data elements as described in Table 22: PA Review Results Response Data Elements for XDR.

Refer to Section 10.7 Information Contained in the PA Review Results Response for XDR or the sample PA Review Response Layout.

Table 22: PA Review Results Response Data Elements for XDR

No.	Data Element Name	Format	Length	Required	Values	Field Description
1.	Content Type Code	Numeric	2	Yes	8, 8.1, and 8.2	The value of this code indicates the line of business. For example, the value '8' indicates a PMD PA request, '8.1' indicates a Non-Emergent Ambulance Transport PA and '8.2' for Hyperbaric Oxygen PA. The Content Type Code is sent by the HIHs in the submission request and is passed all the way to the RCs. The esMD returns the code back in the PA review results response message.

No.	Data Element Name	Format	Length	Required	Values	Field Description
2.	TransactionID	Numeric	10	Yes	Assigned by the esMD	TransactionID is generated by the esMD Gateway when a PA request is received from the HIH Gateway. The TransactionID is sent to the RCs. The RCs shall send the TransactionID back in the PA review results response message.
3.	Decision Indicator	Char	1	Yes	Either of the four possible values: A, N, M or R	The value of this data element shall indicate whether a PA request has been Affirmed (A), Non-affirmed (N), Modified(M) or Rejected (R)
4	Number of Units Approved	Numeric	10	Situational	Assigned by RC	The value of this data element shall indicate the modified value of units approved by RC for Non-Emergent Ambulance Transport and HBO PA programs.
5	Approved Service Date	Date (MM-DD-YYYY) (Note: To be updated in a future version of this guide.)	N/A	Situational	Assigned by RC	The value of this data element shall indicate the date for which the service is approved by RC for Non-Emergent Ambulance Transport and Hyperbaric Oxygen PA programs.
6	Approved Service Date Range(Start Date and End Date)	Date (MM-DD-YYYY)	N/A	Situational	Assigned by RC	The value of this data element shall indicate the date range (start date and end date) for which the service is approved by RC for Non-Emergent Ambulance Transport and HBO PA programs.

No.	Data Element Name	Format	Length	Required	Values	Field Description
7	Unique Tracking Number (UTN)	String	64	Situational	Assigned by RC	A unique tracking number assigned by the RCs. This number is used by the provider/RC supplier to file a claim with the CMS.
8.	Reason Identifier (DEN Code)	String	12	Situational	example: PMD1A	A coded value to indicate which coverage criterion or documentation requirements was not met by the provider/RC Supplier. There can be multiple reason identifiers for a single response sent by RC to the HIH.

10.3 Rules about Situational Data Elements in the PA Review Results Response

As noted in Table 22: PA Review Results Response Data Elements for XDR above, few data elements in the PA review results response are situational. Based on the value of the Decision Indicator, the values of Number of Approved Units, Approved Date, Approved Date Range (Start Date and End Date), Unique Tracking Number (UTN) and Reason Identifier shall be governed.

Note: PMD PA Review results response shall not have the Modified (“M”) decision in the response send by the RC.

10.3.1 Situational Data Elements for Affirmed Decision

Table 23: Affirmed PA Review Results Responses elaborates the situation data elements for an affirmed decision in the PA review results response.

Table 23: Affirmed PA Review Results Responses

No.	Rule
1.	Affirmed (A) PA review results responses shall contain a Unique Tracking Number (UTN) assigned by the RCs.
2.	Affirmed (A) PA review results responses shall not contain Number of Approved Units.
3.	Affirmed (A) PA review results responses shall not contain either Approved Date or Approved Date Range (Start Date and End Date).

No.	Rule
4.	Affirmed (A) PA review results responses shall not contain Reason Identifier(s).

10.3.2 Situational Data Elements for Non-Affirmed Decision

Table 24: Non-Affirmed PA Review Results Responses elaborates the situation data elements for an affirmed decision in the PA review results response.

Table 24: Non-Affirmed PA Review Results Responses

No.	Rule
1.	Non-affirmed (N) PA review results responses shall contain a Unique Tracking Number (UTN) provided by the RCs.
2.	Non-Affirmed (N) PA review results responses shall not contain Number of Approved Units.
3.	Non-Affirmed (N) PA review results responses shall not contain either Approved Date or Approved Date Range (Start Date and End Date).
4.	Non-affirmed (N) PA review results responses shall contain Reason Identifier(s) provided by the RCs.

10.3.3 Situational Data Elements for Modified Decision

Table 25: Modified PA Review Results Responses elaborates the situation data elements for an affirmed decision in the PA review results response.

Table 25: Modified PA Review Results Responses

No.	Rule
1.	Modified (M) PA review results responses shall contain a Unique Tracking Number (UTN) provided by the RCs.
2.	Modified (M) PA review results responses shall contain Number of Approved Units.
3.	Modified (M) PA review results responses shall contain either Approved Date or Approved Date Range (Start Date and End Date).
4.	Modified (M) PA review results responses shall contain Reason Identifier(s) provided by the RCs.

10.3.4 Situational Data Elements for Rejected Decision

Table 26: Rejected PA Review Results Responses elaborates the situation data elements for an affirmed decision in the PA review results response.

Table 26: Rejected PA Review Results Responses

No.	Rule
1.	Rejected (R) PA review results responses shall contain a Unique Tracking Number (UTN) provided by the RCs.
2.	Rejected (R) PA review results responses shall not contain Number of Approved Units.
3.	Rejected (R) PA review results responses shall not contain either Approved Date or Approved Date Range (Start Date and End Date).
4.	Rejected (R) PA review results responses shall contain Reason Identifier(s).

10.4 Note on Reason Identifier (DEN Code)

In a single Non-affirmed (N), Modified (M) or Rejected (R) PA review results response, the RCs can send more than one Reason Identifier (DEN Code). It is possible for the RCs to send a maximum of up to 25 Reason Identifiers in a single Non-affirmed, Modified or Rejected PA review results response.

Refer to Appendix G: PA Reason Identifiers and Statements for further information.

10.5 Rules about Unique Tracking Number in PA Review Results Response

In a single PA Review Result Response or PA Error Response, the unique tracking number value should follow the rules as described in Table 27: UTNs in PA Review Results Responses.

Table 27: UTNs in PA Review Results Responses

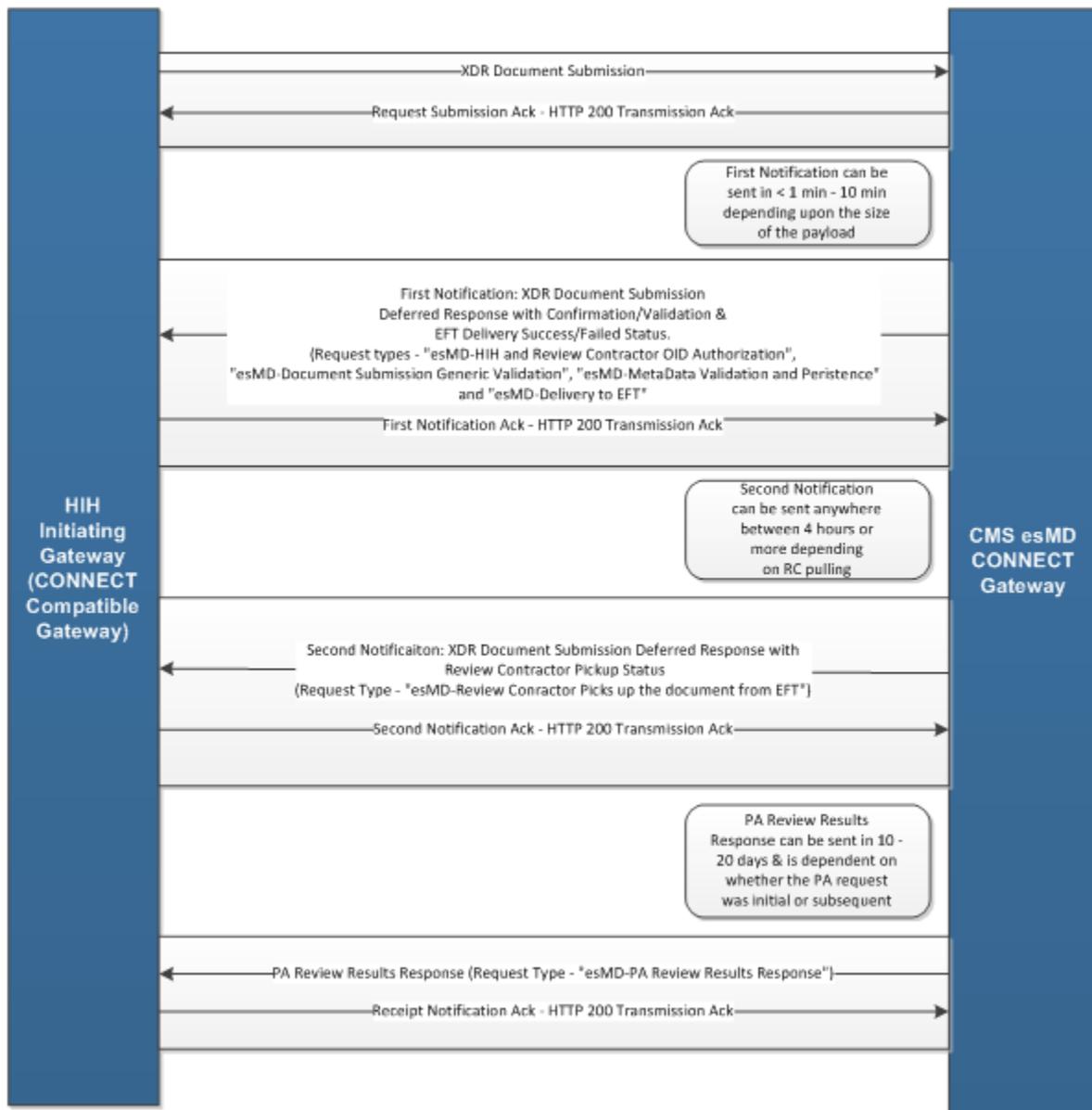
No.	Rule
1.	For a single Affirmed (A), Non-Affirmed (N) or Affirmed with a Change (M) PA Review Result Response, a unique tracking number must be provided. A unique tracking number must be a minimum of 1 and a maximum of 50 alphanumeric characters long.
2.	For a single Rejected (R) Error Response, unique tracking number may or may not be provided. A unique tracking number must be a minimum of 1 and a maximum of 50 alphanumeric characters long.

10.6 Status and Notification Messages for PA

In Figure 10: Outbound Response Notification, the very last response refers to the outbound (i.e., from the esMD Gateway to HIH) PA Review Results Response and was the new functionality for the esMD Release 2.0.

Note: The First and Second Notifications depicted in Figure 10: Outbound Response Notification are existing notifications sent in response to inbound submissions to the esMD Gateway from the HIHs. Please refer to Section 8, XDR Status and Notification Messages and Section 9, The esMD System CAQH Profile for more information on the existing notifications.

Figure 10: Outbound Response Notification



10.7 Information Contained in the PA Review Results Response for XDR

HIHs should look for the following information in the response message: MessageID, UniqueID, Request ID, Status, and Response Slots.

10.7.1 MessageID (Shall be Correlated with PA Request Message ID)

To correlate the PA review results response with the PA request sent by the HIHs, the MessageID sent by the HIHs in the PA request shall be returned in the response message. The MessageID is described in the example below.

<ns20:assertion>


```
<ns19:samlAuthnStatement>
  <ns19:authInstant>2009-04-16T13:15:39Z</ns19:authInstant>
  <ns19:sessionIndex>987</ns19:sessionIndex>
```

```
<ns19:authContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</ns19:authContextClassRef>
```

```
  <ns19:subjectLocalityAddress>158.147.185.168</ns19:subjectLocalityAddress>
  <ns19:subjectLocalityDNSName>esmdval.cms.hhs.gov</ns19:subjectLocalityDNSName>
</ns19:samlAuthnStatement>
<ns19:samlAuthzDecisionStatement>
  <ns19:decision>Permit</ns19:decision>
```

```
<ns19:resource>https://158.147.185.168:8181/SamlReceiveService/SamlProcessWS</ns19:resource>
```

```
  <ns19:action>TestSaml</ns19:action>
  <ns19:evidence>
    <ns19:assertion>
      <ns19:id>esMDQSSI_NM_04042013_ADMC_11</ns19:id>
      <ns19:issueInstant>2009-04-16T13:10:39.093Z</ns19:issueInstant>
      <ns19:version>2.0</ns19:version>
      <ns19:issuer>CN=SAML
        User,OU=Harris,O=HITS,L=Melbourne,ST=FL,C=US</ns19:issuer>
      <ns19:issuerFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</ns19:issuerFormat>
      <ns19:conditions>
        <ns19:notBefore>2009-04-16T13:10:39.093Z</ns19:notBefore>
        <ns19:notOnOrAfter>2009-12-31T12:00:00.000Z</ns19:notOnOrAfter>
      </ns19:conditions>
```

```
<ns19:accessConsentPolicy>urn:oid:2.16.840.1.113883.13.34.110.3</ns19:accessConsentPolicy>
```

```
<ns19:instanceAccessConsentPolicy>urn:oid:2.16.840.1.113883.13.34.110.3</ns19:instanceAccessC
onsentPolicy>
  </ns19:assertion>
</ns19:evidence>
</ns19:samlAuthzDecisionStatement>
  <ns19:messageId>uuid:4e0903af-4145-42b1-a06b-45381786bf1c</ns19:messageId>
</ns20:assertion>
```

10.7.2 UniqueID (Shall Be Correlated with PA Request Unique ID)

To correlate the PA review results response with the PA request sent by the HIHs, the UniqueID sent by the HIHs in the PA request shall be copied back in the response message. The UniqueID is described in the example below.

```
<urn1:samlAuthzDecisionStatement>
  -----
  <urn1:evidence>
    <urn1:assertion>
      <urn1:id>esMDQSSI_NM_04042013_ADMC_11</urn1:id>
      -----
    </urn1:assertion>
  </urn1:evidence>
</urn1:samlAuthzDecisionStatement>
```

10.7.3 RequestID

The RequestID explains the type of response Type. Table 28: PA Outbound Request Type lists the request type string that shall be used for PA outbound.

Table 28: PA Outbound Request Type

No.	Request Type String	Request Type in Response Messages
1.	"esMD- PA Review Results Response"	PA Review Results Response

```
<ns20:RegistryResponse
  requestId="esMD - PA Review Results Response"
  status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  <ns10:ResponseSlotList>
    ----
    ---
  </ns10:ResponseSlotList>
</ns20:RegistryResponse>
```

10.7.4 Status

Refer to the section 8.5.4 Status for the description of this section.

10.7.5 Response Slots

The PA review results response specific slots shall have the response specific information. The following shall be the slots:

1. creationTime
2. submissionTime
3. esMDTransactionId
4. contentTypeCode
5. DecisionIndicator
6. approvedUnits
7. approvedDate
8. Approved Date Range (approvedStartDate and approvedEndDate)
9. uniqueTrackingNumber
10. ReasonIdentifierDtIs

10.7.5.1 Creation Time Response Slot

Below is the example of creation time response slot:

```
<ns5:Slot name="creationTime">  
  <ns5:ValueList>  
    <ns5:Value>2015-07-21T08:41:29.119-04:00</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.2 Submission Time Response Slot

Below is an example of the esMD's submission time response slot:

```
<ns5:Slot name=" submissionTime">  
  <ns5:ValueList>  
    <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.3 The esMD Transaction Id Response Slot

Below is an example of the esMD's Transaction Id response slot:

```
<ns5:Slot name="esMDTransactionId">  
  <ns5:ValueList>  
    <ns5:Value>12812678</ns5:Value>
```

```
</ns5:ValueList>  
</ns5:Slot>
```

10.7.5.4 The esMD Content Type Code Response Slot

Below is an example of the esMD's Content Type Code response slot:

```
<ns5:Slot name="contentTypeCode">  
  <ns5:ValueList>  
    <ns5:Value>8</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.5 Decision Indicator Response Slot

Below is an example of the esMD's decision indicator response slot:

```
<ns5:Slot name="PMDDDecisionIndicator">  
  <ns5:ValueList>  
    <ns5:Value>A</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.6 Approved Units Response Slot

Below is an example of the esMD's approved unit's response slot:

```
<ns5:Slot name="approvedUnits">  
  <ns5:ValueList>  
    <ns5:Value>12</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.7 Approved Date Response Slot

Below is an example of the esMD's approved date response slot:

```
<ns5:Slot name="approvedDate">  
  <ns5:ValueList>  
    <ns5:Value>02/18/2015</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

10.7.5.8 Approved Date Range Response Slot

Below is an example of the esMD's approved date range response slot:

```
<ns5:Slot name="approvedStartDate">  
  <ns5:ValueList>  
    <ns5:Value>02/16/2015</ns5:Value>
```

```
</ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="approvedEndDate">
  <ns5:ValueList>
    <ns5:Value>02/26/2015</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
```

10.7.5.9 Unique Tracking Number Response Slot

Below is an example of the esMD's unique tracking number response slot:

```
<ns5:Slot name="uniqueTrackingNumber">
  <ns5:ValueList>
    <ns5:Value>A0014280106600</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
```

10.7.5.10 Reason Identifier Response Slot

ReasonIdentifierDtIs is a list of objects and shall have the Reason Identifier, as a child element:

```
<ns5:Slot name="ReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD1Z</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="ReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD2Z</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
```

In the above example, the complex data type "ReasonIdentifierDtIs" has one child slot:

- The value of the first slot shall carry the Reason Identifier (DEN Code). In the example above, it is:
 - PMD1Z; and
 - PMD2Z.

It is important to note that based on the rules mentioned in section 10.3 Rules about Situational Data Elements in the PA Review Results Response, the values of situational data elements should be governed. If a situational value is not present, the xml tag carrying it will not be present in the PA review results response sent by the esMD Gateway to the HIH.

10.8 Sample Outbound PA Review Results Responses for XDR

10.8.1 Affirmed PA Review Results Response

A complete outbound affirmed PA review results response is shown below:

```
<ns17:RegistryResponse requestId="esMD - PA Review Results Response"  
status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
```

```
<ns6:ResponseSlotList>  
  <ns5:Slot name="creationTime">  
    <ns5:ValueList>  
      <ns5:Value>2015-07-21T08:41:29.119-04:00</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="submissionTime">  
    <ns5:ValueList>  
      <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="esMDTransactionId">  
    <ns5:ValueList>  
      <ns5:Value>12812678</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="contentTypeCode">  
    <ns5:ValueList>  
      <ns5:Value>8</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="uniqueTrackingNumber">  
    <ns5:ValueList>  
      <ns5:Value>R4567</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>
```

```
<ns5:Slot name="PADecisionIndicator">  
  <ns5:ValueList>  
    <ns5:Value>A</ns5:Value>  
  </ns5:ValueList>  
</ns5:Slot>
```

```
</ns6:ResponseSlotList>  
</ns17:RegistryResponse>
```

10.8.2 Non-Affirmed PA Review Results Response

An excerpt of a Non-Affirmed outbound PA review results response is shown below:

```
<ns17:RegistryResponse requestId="esMD - PA Review Results Response"  
status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
```

```
<ns6:ResponseSlotList>  
  <ns5:Slot name="creationTime">  
    <ns5:ValueList>  
      <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="submissionTime">  
    <ns5:ValueList>  
      <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="esMDTransactionId">  
    <ns5:ValueList>  
      <ns5:Value>12345678</ns5:Value>  
    </ns5:ValueList>  
  </ns5:Slot>  
  <ns5:Slot name="contentTypeCode">  
    <ns5:ValueList>  
      <ns5:Value>8.1</ns5:Value>
```

```
</ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="uniqueTrackingNumber">
  <ns5:ValueList>
    <ns5:Value>A0014280106600</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PADecisionIndicator">
  <ns5:ValueList>
    <ns5:Value>N</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>AMB2M</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>AMB4B</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>AMB2Z</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>AMB3Q</ns5:Value>
  </ns5:ValueList>
```

```

</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>AMB4P</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
</ns6:ResponseSlotList>
</ns17:RegistryResponse>

```

10.8.3 The esMD Modified PA Review Results Response

An excerpt of a modified outbound PA review results response is shown below:

```

<ns17:RegistryResponse requestId="esMD - PA Review Results Response"
status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  <ns6:ResponseSlotList>
    <ns5:Slot name="creationTime">
      <ns5:ValueList>
        <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name=" submissionTime">
      <ns5:ValueList>
        <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="esMDTransactionId">
      <ns5:ValueList>
        <ns5:Value>12812678</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="contentTypeCode">
      <ns5:ValueList>
        <ns5:Value>8.2</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="uniqueTrackingNumber">
      <ns5:ValueList>
        <ns5:Value>A0014280107809</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="PADecisionIndicator">
      <ns5:ValueList>
        <ns5:Value>M</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="approvedUnits">
      <ns5:ValueList>
        <ns5:Value>12</ns5:Value>
      </ns5:ValueList>
    </ns5:Slot>
  </ns6:ResponseSlotList>
</ns17:RegistryResponse>

```

```

        </ns5:ValueList>
    </ns5:Slot>
    <!--If Approved Date is the only date to be sent, use this slot -->
    <ns5:Slot name="approvedDate">
        <ns5:ValueList>
            <ns5:Value>02/18/2015</ns5:Value>
        </ns5:ValueList>
    </ns5:Slot>
    <!--If Approved Start Date and the Approved End Date are to be sent -
->
    <ns5:Slot name="approvedStartDate">
        <ns5:ValueList>
            <ns5:Value>02/16/2015</ns5:Value>
        </ns5:ValueList>
    </ns5:Slot>
    <ns5:Slot name="approvedEndDate">
        <ns5:ValueList>
            <ns5:Value>02/26/2015</ns5:Value>
        </ns5:ValueList>
    </ns5:Slot>
</ns6:ResponseSlotList>
</ns17:RegistryResponse>

```

10.8.4 The esMD Rejected PA Review Results Response

An excerpt of a rejected outbound PA review results response is shown below:

```

<ns17:RegistryResponse requestId="esMD - PA Review Results Response"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
    <ns6:ResponseSlotList>
        <ns5:Slot name="creationTime">
            <ns5:ValueList>
                <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>
            </ns5:ValueList>
        </ns5:Slot>
        <ns5:Slot name="submissionTime">
            <ns5:ValueList>
                <ns5:Value>2015-07-21T08:43:46.009-04:00</ns5:Value>
            </ns5:ValueList>
        </ns5:Slot>
        <ns5:Slot name="esMDTransactionId">
            <ns5:ValueList>

```

```
<ns5:Value>12345678</ns5:Value>
</ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="contentTypeCode">
  <ns5:ValueList>
    <ns5:Value>8</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PADecisionIndicator">
  <ns5:ValueList>
    <ns5:Value>R</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD2Z</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD3A</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD2A</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD5A</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
```

```
</ns5:ValueList>
</ns5:Slot>
<ns5:Slot name="PAReasonIdentifierDtIs">
  <ns5:ValueList>
    <ns5:Value>PMD4A</ns5:Value>
  </ns5:ValueList>
</ns5:Slot>
</ns6:ResponseSlotList>
</ns17:RegistryResponse>
```

11 X12N 278 5010 PA Response

11.1 X12N 278 5010 Review Response Data Elements

Refer to the following link for the X12 Companion Guide for more details on the Data Elements in an X12 Review Response:

https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Information_for_HIHs.html

11.2 X12N 278 5010 Error Response Data Elements

Refer to the following link for the X12 Companion Guide for more details on the Data Elements in an X12 Review Response Error:

https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/Information_for_HIHs.html

12 Retry Functionality

The esMD Gateway shall expect an HTTP 200 acknowledgement back from the HIH Gateway as a receipt of the message for any of the transmissions that are delivered to HIH by the esMD. If the esMD Gateway does not receive an HTTP 200 acknowledgement back, it will retry sending the following transmissions to the HIH Gateway. If the esMD Gateway fails to deliver any of the following transmissions due to unavailability of HIH gateway after the three retries, the esMD will initiate an email communication to the esMD Support team to reach out to HIH/RC manually through phone contact and/or email communication.

12.1 Retry Scenarios Common for Both X12 and XDR Transmissions

Table 29: Retry Scenarios Common for Both X12 and XDR Transmissions provide the retry scenarios that are common for both X12 and XDR transmissions.

Table 29: Retry Scenarios Common for Both X12 and XDR Transmissions

ID	Transmission	1st Retry	2nd Retry	3rd Retry	Retry Failure Scenario
1.	First Notification. See section 8.2.1.1 Success Message Without Warnings for more details.	Retry sending in four hours i.e., after the "HTTP 400" error is received for the first time.	Retry sending in four hours i.e., after the "HTTP 400" error is received for the second time.	Retry sending in four hours i.e., after the "HTTP 400" error is received for the third time.	The esMD sends email to the esMD Support team with HIH's phone contact and email to reach out to them manually to convey the message "".
2.	Second Notification. See for more details	Retry sending in four hours i.e., after the "HTTP 400" error is received for the first time.	Retry sending in four hours i.e., after the "HTTP 400" error is received for the second time.	Retry sending in four hours i.e., after the "HTTP 400" error is received for the third time.	The esMD sends email to the esMD Support team with HIH's phone contact and email to reach out to them manually to convey the message "".

ID	Transmission	1st Retry	2nd Retry	3rd Retry	Retry Failure Scenario
3.	Third Notification for both X12 and XDR PA Requests. See 8.4 The esMD System Third Notification for more details.	Retry sending in four hours i.e., after the “HTTP 400” error is received for the first time.	Retry sending in four hours i.e., after the “HTTP 400” error is received for the second time.	Retry sending in four hours i.e., after the “HTTP 400” error is received for the third time.	The esMD sends email to the esMD Support team with RC’s phone contact and email to reach out to them manually to convey the message “Resubmit the decision response”.
4.	Any other error message	Retry sending in four hours i.e., after the “HTTP 400” error is received for the first time.	Retry sending in four hours i.e., after the “HTTP 400” error is received for the second time.	Retry sending in four hours i.e., after the “HTTP 400” error is received for the third time.	The esMD sends email to the esMD Support team with HIH’s phone contact and email to reach out to them manually to convey the message “”.

12.2 X12 Retry Scenarios

The Table 30: Retry Scenarios for X12 Transmissions Only describes the retry scenarios for the X12N 278 5010 transmissions only. This does not apply to the XDR transmissions.

Table 30: Retry Scenarios for X12 Transmissions Only

ID	Transmission	1 st Retry	2 nd Retry	3 rd Retry	Retry Failure Scenario
1.	A 2-Business Day notification	Retry sending in four hours, i.e. after the "HTTP 400" error is received for the first time.	Retry sending in four hours, i.e. after the "HTTP 400" error is received for the second time.	Retry sending in four hours, i.e. after the "HTTP 400" error is received for the third time.	The esMD sends an email to the esMD Support team with HIH's phone contact and email to reach out to them manually to convey the message "Missing documentation must be submitted quickly."
2.	A 4-Business Day Reject notification	Retry sending in four hours, i.e. after the "HTTP 400" error is received for the first time.	Retry sending in four hours, i.e., after the "HTTP 400" error is received for the second time.	Retry sending in four hours, i.e. after the "HTTP 400" error is received for the third time.	The esMD sends an email to the esMD Support team with HIH's phone contact and email to reach out to them manually to convey the message "The Request has been rejected and a new request and documentation to be resubmitted".

13 The esMD Reports to HIH

The esMD system sends the daily transaction reports to each HIH, including all XDR and X12 submissions, excluding the additional documentation sent for X12 transactions. The daily transaction reports are sent in PDF format to each HIH.

Table 31: HIH Daily Transaction Report and Table 32: HIH Daily Transaction Report in Excel Format show all the data elements sent as part of the daily transaction report.

Table 31: HIH Daily Transaction Report in PDF format

Home ▾ Tools ▾ Data ▾ Last update: 8/4/15 5:35:10														
														
Legend HIH														
Transaction	Submission Date	CTC ID	CTC DESC	CTC PA_FLAG_XDR_>	Transact Status	HIH	Review Contractor	Unique ID	RC Pickup Time	RC/PA Response Time	Number Of Documents	Failure Reason	RC Pickup Status	Delivery to EFT
1097585	7/23/2015 5:51 PM	1	Response to Additional Documentati Request (ADR)	XDR	Failure	LOISS	RAC D HDI	3.32.41145.20150			1			
1098534	7/28/2015 10:54 PM	1	Response to Additional Documentati Request (ADR)	XDR	Failure	LOISS	RAC D HDI	3.32.41145.20150			1			
1098535	7/28/2015 11:07 PM	1	Response to Additional Documentati Request (ADR)	XDR	Failure	LOISS	RAC D HDI	3.32.41145.20150			1			
1098983	7/29/2015 7:43 PM	1	Response to Additional Documentati Request (ADR)	XDR	Failure	LOISS	RAC D HDI	3.32.41145.20150			1			

Table 32: HIH Daily Transaction Report in Excel Format

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Transacti	Submission Date	CTC	CTC	CTC	Transaction Status	HIH	Review	Unique ID	RC Pickup Time	RC/PA Response	Number	Failure	RC Pickup Status	Delivery to EFT
2604833	5/11/2016 11:21 AM	1	Response	XDR	Document Sent to	MedFORCE	DME MAC C CGS	43082C2B-A2A9-48BC-9209-AD3EE70AF54A			1	ESMD TO		
2602905	5/10/2016 3:29 PM	8	PMD PA	XDR-PA	Failure	MedFORCE	DME MAC C CGS	62FC0756-A6A3-4466-9449-2941B3DD7CEA			1	INBOUND NPI		
2582854	4/29/2016 10:24 AM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC D Noridian	A57516AA-F8BE-4F2A-A66A-AE5EA78D5C2A	#####	5/10/2016 4:35:28 PM	1		PICKUP NOTIFICATION	4/29/2016 10:24:21 AM
2585644	5/2/2016 10:43 AM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC C CGS	CFDC3B50-51D2-49C0-9993-E1793D17BB28	5/2/2016 11:34:24 AM	5/10/2016 7:32:27 PM	1		PICKUP NOTIFICATION	5/2/2016 10:43:07 AM
2585742	5/2/2016 11:14 AM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC D Noridian	C4AE6E64-1886-4FF0-B707-4E226FF1C285	5/2/2016 11:27:13 AM	5/10/2016 4:35:28 PM	1		PICKUP NOTIFICATION	5/2/2016 11:14:11 AM
2586755	5/2/2016 3:33 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC C CGS	3A2F9390-7D2D-4361-9249-49A502611B10	5/2/2016 4:01:16 PM	5/10/2016 3:25:26 PM	1		PICKUP NOTIFICATION	5/2/2016 3:33:08 PM
2586764	5/2/2016 3:34 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC C CGS	3602C68C-C6C0-4E66-8290-C9358AAC9C15	5/2/2016 4:01:46 PM	5/10/2016 9:18:26 AM	1		PICKUP NOTIFICATION	5/2/2016 3:34:10 PM
2588717	5/3/2016 12:49 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC C CGS	CABF75FC-C44A-445D-9A69-99CA8DF28C09	5/3/2016 2:18:18 PM	5/10/2016 11:19:38 AM	1		PICKUP NOTIFICATION	5/3/2016 12:49:43 PM
2589416	5/3/2016 3:19 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC C CGS	3D835A53-055B-4E42-AF47-5FA26ACBF916	5/3/2016 4:36:54 PM	5/10/2016 1:24:29 PM	1		PICKUP NOTIFICATION	5/3/2016 3:19:20 PM
2593646	5/5/2016 9:14 AM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC A NHC	067699C5-B6AD-464E-BA77-B9DD4594BAB8	5/5/2016 9:19:43 AM	5/10/2016 3:39:26 PM	1		PICKUP NOTIFICATION	5/5/2016 9:14:09 AM
2594588	5/5/2016 1:46 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC B NGS	849D0BEC-4650-4020-BD43-F42D4755C503	5/5/2016 1:50:47 PM	5/10/2016 8:52:28 AM	1		PICKUP NOTIFICATION	5/5/2016 1:46:12 PM
2594943	5/5/2016 3:12 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC B NGS	7EF2804C-B124-4AAB-BD09-20E78D55A4E8	5/5/2016 3:16:27 PM	5/10/2016 8:58:27 AM	1		PICKUP NOTIFICATION	5/5/2016 3:12:30 PM
2595326	5/5/2016 4:18 PM	8	PMD PA	XDR-PA	Sent PA Review Results HIH ACK to RC	MedFORCE	DME MAC B NGS	E7E839A3-8723-4147-9025-F2980155E24A	5/5/2016 4:23:23 PM	5/10/2016 9:02:26 AM	1		PICKUP NOTIFICATION	5/5/2016 4:18:08 PM

14 GLOSSARY

Term	Definition
Acknowledgement (ACK)	Message (such as one used in 'handshaking' process between two systems) that indicates the status of communications received. It is commonly written as ACK.
Additional Documentation Request (ADR)	Official letters sent to providers from the CMS RCs requesting additional documentation that is needed to process claims.
Advanced Determination of Medical Coverage (ADMC)	A voluntary program that allows Suppliers and Beneficiaries to request prior approval of eligible items (e.g., wheelchairs) before delivery of the items to the beneficiary.
ANSI	American National Standards Institute
ASC	Accredited Standards Committee
CAQH	Council for Affordable Quality Healthcare
CORE	Committee on Operating Rules for Information Exchange
CONNECT	CONNECT implements a flexible, open-source gateway solution that enables healthcare entities - Federal agencies or private-sector health organizations or networks - to connect their existing health information systems to the eHealth Exchange. CONNECT is fully functional out-of-the-box, while at the same time configurable and flexible to allow organizations to customize it to meet their needs and those of their existing health information systems.
De-identified Data	De-identified data is data from which patient identifiers consisting of Personally Identifiable Information (PII) is removed. The business rules for de-identified data follow the HIPAA Privacy Rule including the de-identification of the specified identifiers.
Electronic Submission of Medical Documentation (esMD)	A new mechanism for submitting medical documentation via a secure Internet gateway connecting providers to the Centers for Medicare & Medicaid Services (CMS). In its second phase, the esMD will allow Medicare RCs to electronically submit claim related Additional Document Request (ADR) letters, and other use case requests, to providers when their claims are selected for review.

Term	Definition
Health Information Handler (HIH)	A Health Information Handler (HIH) is defined as an organization that oversees and governs the exchange of health-related claim reviewer information from provider to the esMD Gateway according to nationally recognized standards.
Health Information Technology Standards Panel (HITSP)	HITSP is a volunteer-driven, consensus-driven organization that is sponsored through a contract from the Department of Health and Human Services (HHS). HITSP harmonizes and recommends the technical standards that are crucial to assure the interoperability of electronic health records.
HTTPS	A set of rules for a speedy retrieval and transmission of electronic documents written in HTML over a secure connection. HTTPS addresses differentiated from HTTP because they encrypt and decrypt user pages to prevent unauthorized access to sensitive data. Online credit card processing and banking websites use HTTPS addresses to ensure privacy and provide secure processing for users.
Interoperability	Interoperability is the ability of health information systems to work together, within and across organizational boundaries, in order to advance the effective delivery of healthcare for individuals and communities.
Interface	A well-defined boundary where direct contact between two different environments, systems, etc., occurs, and where information is exchanged.
eHealth Exchange	The eHealth Exchange is a set of standards, protocols, legal agreements, and specifications that a consortium of health information organizations have agreed are necessary for secure and private exchange of health information over the Internet. The eHealth Exchange is overseen by the Office of the National Coordinator for Health IT (ONC).
Performance	Accomplishment of a transaction measured against preset standards of accuracy, completeness, cost, and speed.
Privacy	An individual's interest in protecting his or her individually identifiable health information and the corresponding obligation of those persons and entities, that participate in a network for the purposes of electronic exchange of such information, to respect those interests through fair information practices.

Term	Definition
Power Mobility Device (PMD) Prior Authorization (PA)	The CMS implemented a Prior Authorization process for scooters and power wheelchairs for people with Fee-For-Service Medicare who reside in seven states with high populations of fraud- and error-prone providers (CA, IL, MI, NY, NC, FL, and TX). This demonstration will help ensure that a beneficiary's medical condition warrants their medical equipment under existing coverage guidelines. Moreover, the program will assist in preserving a Medicare beneficiary's ability to receive quality products from accredited suppliers.
Response Time	It is the interval between a user-command and the receipt of an action, result, or feedback from the system. It is expressed as the sum of (a) transmission time of the command to the system, (b) processing time at the CPU, (c) access time to obtain required data from a storage device, and (d) transmission time of the result back to the user. When applied to a system component, it is the time taken to react to a system request or a given input.
SAML	Security Assertion Markup Language used for message authentication.
Security	The physical, technological, and administrative safeguards used to protect individually identifiable health information.
SOAP	Simple Object Access Protocol is a message exchange format for web services.

TLS	<p>Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that "provide communications security over the Internet". TLS and SSL encrypt the segments of network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability. TLS is an IETF standards track protocol, last updated in RFC 5246, and based on the earlier SSL specifications developed by Netscape Corporation.</p> <p>The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. A TLS client and server negotiate a successful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security.</p> <ul style="list-style-type: none">• The handshake begins when a client connects to a TLS-enabled server requesting a secure connection, and presents a list of supported CipherSuites (ciphers and hash functions).• From this list, the server picks the strongest cipher and hash function that it supports and notifies the client of the decision.• The server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA), and the server's public encryption key.• The client may contact the server that issued the certificate (the trusted CA as above) and confirm that the certificate is valid before proceeding.• In order to generate the session keys used for the secure connection, the client encrypts a random number (RN) with the server's public key (PbK), and sends the result to the server. Only the server should be able to decrypt it (with its private key (PvK)): this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data. The client knows PbK and RN, and the server knows PvK and (after decryption of the client's message) RN. A third party is only able to know RN if PvK has been compromised.• From the random number, both parties generate key material for encryption and decryption.
-----	--

Term	Definition
TLS (Cont.)	<ul style="list-style-type: none"><li data-bbox="602 331 1388 436">• This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the key material until the connection closes. <p data-bbox="553 449 1388 512">If any one of the above steps fails, the TLS handshake fails, and the connection is not created.</p>
Transaction	Event or process (such as an input message) initiated or invoked by a user or system, regarded as a single unit of work and requiring a record to be generated for processing in a database.

15 ACRONYMS

Acronym	Term
ACN	Attachment Control Number
ADMC	Advanced Determination of Medical Coverage
ADR	Additional Documentation Request
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASC	Accredited Standards Committee
CA	Certificate Authority
CAQH	Council for Affordable Quality Healthcare
CDA	Clinical Document Architecture
CCHIT	Certification Commission for Health Information Technology
CMS	Centers for Medicare & Medicaid Services
CERT	Comprehensive Error Rate Testing
CORE	Committee on Operating Rules for Information Exchange
DEN	Denial Code
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics, and Supplies
DNS	Domain Name System
EHR	Electronic Health Record
esMD	Electronic Submission of Medical Documentation
FFS	Fee-For-Service
FIPS	Federal Information Processing Standards

Acronym	Term
HBO	Hyperbaric Oxygen
HHS	U.S. Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Information Portability and Accountability Act
HIT	Health Information Technology
HITSP	Health Information Technology Standards Panel
HL7	Health Level 7
HIH	Health Information Handler
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IHE	Integrating the Healthcare Enterprise
IP	Internet Protocol
MAC	Medicare Audit Contractor
MIC	Medicaid Integrity Contractor
MIME	Multi-Purpose Internet Mail Extensions
MTOM	Message Transmission Optimization Mechanism
NAT	Network Address Translation
NHIN	Nationwide Health Information Network
NIST	National Institute of Standards and Technology
NPI	National provider Identifier

Acronym	Term
OASIS	Organization for the Advancement of Structured Information Standards
OID	Organizational Identification
ONC	Office of National Coordinator for HIT
PDF	Portable Document Format
PERM	Program Error Rate Measurement
PMD PA	Power Mobility Device Prior Authorization
RC	Review Contractor
RA	Recovery Auditors
ROI	Release of Information
RHIO	Regional Health Information Organization
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTN	Unique Tracking Number
XDR	External Data Representation
XML	Extensible Markup Language
ZPIC	Zone Program Integrity Contractor

Appendix A. SOAP Message For Inbound (HIH To CMS) Submissions

Sample SOAP Message (the values will be different based on the use case).

The message provided below is a response to ADR and is sent to MAC J9.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
  xmlns:urn="urn:gov:hhs:fha:nhinc:common:nhinccomponententity"
  xmlns:urn1="urn:gov:hhs:fha:nhinc:common:nhinccommon"
  xmlns:add="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:urn2="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0" xmlns:urn3="urn:oasis:names:tc:ebxml-
  regrep:xsd:rs:3.0" xmlns:urn4="urn:oasis:names:tc:ebxml-regrep:xsd:rjm:3.0"
  xmlns:urn5="urn:ihe:iti:xds-b:2007">
  <soapenv:Header/>
  <soapenv:Body projectName="EndToEndSelfTest" testCase="XDR Async">
    <urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>
      <urn:assertion>
        <urn1:homeCommunity>
          <urn1:description>${#Project#LocalHCDescription}</urn1:description>
          <urn1:homeCommunityId>${#Project#LocalHCID}</urn1:homeCommunityId>
          <urn1:name>${#Project#LocalHCDescription}</urn1:name>
        </urn1:homeCommunity>
        <urn1:uniquePatientId>urn:oid:2.16.840.1.113883.13.34.110.1.110.9</urn1:uniquePatientId>
        <urn1:userInfo>
          <urn1:userName>1234567899</urn1:userName>
          <urn1:org>
            <urn1:description>${#Project#LocalHCDescription}</urn1:description>
            <urn1:homeCommunityId>${#Project#LocalHCID}</urn1:homeCommunityId>
            <urn1:name>${#Project#LocalHCDescription}</urn1:name>
          </urn1:org>
        </urn1:userInfo>
        <urn1:organizationId>
          <urn1:description>Description of Broker Organization between provider and the
          submitting HIH CONNECT or CONNECT Compatible Gateway</urn1:description>
        </urn1:organizationId>
      </urn:assertion>
    </urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

```

    <urn1:homeCommunityId>urn:oid:1.3.6.1.4.1.101420.6.1</urn1:homeCommunityId>
    <urn1:name>Name of Broker Organization between provider and the submitting HIH
CONNECT or CONNECT Compatible Gateway</urn1:name>
  </urn1:organizationId>
  <urn1:purposeOfDisclosureCoded>
    <urn1:code>PAYMENT</urn1:code>
    <urn1:codeSystem>2.16.840.1.113883.3.18.7.1</urn1:codeSystem>
    <urn1:codeSystemName>esMD CMS Purpose</urn1:codeSystemName>
    <urn1:codeSystemVersion>1.0</urn1:codeSystemVersion>
    <urn1:displayName>Medical Claim Documentation Review</urn1:displayName>
    <urn1:originalText>Medical Claim Documentation Review</urn1:originalText>
  </urn1:purposeOfDisclosureCoded>
  <urn1:samlAuthnStatement>
    <urn1:authInstant>2011-01-05T16:50:01.011Z</urn1:authInstant>
    <urn1:sessionIndex>987</urn1:sessionIndex>

<urn1:authContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</urn1:authContextClassRe
f>
    <urn1:subjectLocalityAddress>158.147.185.168</urn1:subjectLocalityAddress>
    <urn1:subjectLocalityDNSName>cms.hhs.gov</urn1:subjectLocalityDNSName>
  </urn1:samlAuthnStatement>
  <urn1:samlAuthzDecisionStatement>
    <urn1:decision>Permit</urn1:decision>

<urn1:resource>https://158.147.185.168:8181/esMD/DocumentSubmission</urn1:resource>
  <urn1:action>TestSaml</urn1:action>
  <urn1:evidence>
    <urn1:assertion>
      <urn1:id>cms_esMD_hihname_09172012_VAL_ADR_1</urn1:id>
      <urn1:issueInstant>2011-01-05T16:50:01.011Z</urn1:issueInstant>
      <urn1:version>2.0</urn1:version>
      <urn1:issuerFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</urn1:issuerFormat>

```

```

    <urn1:issuer>CN=HIH SAML
User,OU=QSSI,O=QSSI,L=Baltimore,ST=MD,C=US</urn1:issuer>

    <urn1:conditions>
        <urn1:notBefore>2011-01-05T16:50:01.011Z</urn1:notBefore>
        <urn1:notOnOrAfter>2011-01-05T16:53:01.011Z</urn1:notOnOrAfter>
    </urn1:conditions>

    <urn1:accessConsentPolicy>Claim-Ref-1234 NA for the
esMD</urn1:accessConsentPolicy>

        <urn1:instanceAccessConsentPolicy>Claim-Instance-1 NA for the
esMD</urn1:instanceAccessConsentPolicy>
    </urn1:assertion>
</urn1:evidence>
</urn1:samlAuthzDecisionStatement>
</urn:assertion>
<urn:nhinTargetCommunities>
    <urn1:nhinTargetCommunity>
        <urn1:homeCommunity>
            <urn1:description>${#Project#RemoteHCDescription}</urn1:description>
            <urn1:homeCommunityId>${#Project#RemoteHCID}</urn1:homeCommunityId>
            <urn1:name>${#Project#RemoteHCDescription}</urn1:name>
        </urn1:homeCommunity>
    </urn1:nhinTargetCommunity>
</urn:nhinTargetCommunities>
<urn:ProvideAndRegisterDocumentSetRequest>
    <urn2:SubmitObjectsRequest id="999" comment="esMD Claim Document Submission in
response to Review Contractor ADR Letter">
        <urn4:RegistryObjectList>
            <urn4:ExtrinsicObject id="Document01" mimeType="application/pdf"
objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
                <urn4:Classification id="cl01" classificationScheme="urn:uuid:93606bcf-9494-43ec-
9b4e-a7748d1a838d" classifiedObject="Document01" nodeRepresentation="author">
                    <urn4:Slot name="authorInstitution">
                        <urn4:ValueList>
                            <urn4:Value>603111</urn4:Value>

```

```
</urn4:ValueList>
</urn4:Slot>
<urn4:Slot name="authorPerson">
  <urn4:ValueList>
    <urn4:Value>603</urn4:Value>
  </urn4:ValueList>
</urn4:Slot>
</urn4:Classification>

<urn4:Description>
  <urn4:LocalizedString value="esMD Claim Document Submission in response to
Review Contractor ADR Letter"/>
</urn4:Description>

<urn4:Classification id="cl03" classificationScheme="urn:uuid:f4f85eac-e6cb-4883-
b524-f2705394840f" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.5.25">
  <urn4:Slot name="confidentialityCode">
    <urn4:ValueList>
      <urn4:Value>V</urn4:Value>
    </urn4:ValueList>
  </urn4:Slot>
  <urn4:Name>
    <urn4:LocalizedString value="Very"/>
  </urn4:Name>
</urn4:Classification>
<urn4:Slot name="creationTime">
  <urn4:ValueList>
    <urn4:Value>20110101165910</urn4:Value>
  </urn4:ValueList>
</urn4:Slot>
```

```
<urn4:Classification id="cl04" classificationScheme="urn:uuid:a09d5840-386c-46f2-
b5ad-9c3699a4309d" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
```

```
  <urn4:Slot name="formatCode">
```

```
    <urn4:ValueList>
```

```
      <urn4:Value>1</urn4:Value>
```

```
    </urn4:ValueList>
```

```
  </urn4:Slot>
```

```
  <urn4:Name>
```

```
    <urn4:LocalizedString value="Scanned PDF Document in CDA C62 Construct"/>
```

```
  </urn4:Name>
```

```
</urn4:Classification>
```

```
<urn4:Classification id="cl06" classificationScheme="urn:uuid:ccccf5598-8b07-4b77-
a05e-ae952c785ead" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
```

```
  <urn4:Slot name="practiceSettingCode">
```

```
    <urn4:ValueList>
```

```
      <urn4:Value>1</urn4:Value>
```

```
    </urn4:ValueList>
```

```
  </urn4:Slot>
```

```
  <urn4:Name>
```

```
    <urn4:LocalizedString value="NA"/>
```

```
  </urn4:Name>
```

```
</urn4:Classification>
```

```
<urn4:Slot name="hash">
```

```
  <urn4:ValueList>
```

```
    <urn4:Value>ad18814418693512b767676006a21d8ec7291e84</urn4:Value>
```

```
  </urn4:ValueList>
```

```
</urn4:Slot>
```

```
<urn4:Classification id="cl05" classificationScheme="urn:uuid:f33fb8ac-18af-42cc-
ae0e-ed0b0bdb91e1" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
```

```
  <urn4:Slot name="healthcareFacilityTypeCode">
```

```
    <urn4:ValueList>
```

```

        <urn4:Value>1</urn4:Value>
    </urn4:ValueList>
</urn4:Slot>
<urn4:Name>
    <urn4:LocalizedString value="Health Information Handler (HIH)"/>
</urn4:Name>
</urn4:Classification>
<urn4:Slot name="languageCode">
    <urn4:ValueList>
        <urn4:Value>en-us</urn4:Value>
    </urn4:ValueList>
</urn4:Slot>
<urn4:slot name="legalAuthenticator">
    <urn4:ValueList>
        <urn4:Value>NA</urn4:Value>
    </urn4:ValueList>
</urn4:slot>
    <urn4:ExternalIdentifier id="ei01" registryObject="Document01"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
value="1234567890123^^^&2.16.840.1.113883.13.34&ISO">
        <urn4:Name>
            <urn4:LocalizedString value="XDSSubmissionSet.patientId"/>
        </urn4:Name>
    </urn4:ExternalIdentifier>
    <urn4:Classification id="cl07" classificationScheme="urn:uuid:f0306f51-975f-434e-
a61c-c59651d33983" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
        <urn4:Slot name="codingScheme">
            <urn4:ValueList>
                <urn4:Value>1</urn4:Value>
            </urn4:ValueList>
        </urn4:Slot>
    <urn4:Name>

```

```

        <urn4:LocalizedString value="Outpatient Evaluation And Management"/>
    </urn4:Name>
</urn4:Classification>
<urn4:Slot name="serviceStartTime">
    <urn4:ValueList>
        <urn4:Value>20110101165910</urn4:Value>
    </urn4:ValueList>
</urn4:Slot>
<urn4:Slot name="serviceStopTime">
    <urn4:ValueList>
        <urn4:Value>20110101165910</urn4:Value>
    </urn4:ValueList>
</urn4:Slot>
<urn4:Slot name="size">
    <urn4:ValueList>
        <urn4:Value>1024000</urn4:Value>
    </urn4:ValueList>
</urn4:Slot>
<urn4:Name>
    <urn4:LocalizedString value="Claim Supporting Medical Documentation"/>
</urn4:Name>
<urn4:Classification id="cl08" classificationScheme="urn:uuid:41a5887f-8865-4c09-
adf7-e362475b143a" classifiedObject="Document01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
    <urn4:Slot name="classCode">
        <urn4:ValueList>
            <urn4:Value>1</urn4:Value>
        </urn4:ValueList>
    </urn4:Slot>
<urn4:Name>
    <urn4:LocalizedString value="Unstructured Document Submission"/>
</urn4:Name>
</urn4:Classification>

```

```

        <urn4:ExternalIdentifier id="ei02" registryObject="Document01"
identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"
value="1.3.6.1.4.1.21367.2005.3.9999.33">
            <urn4:Name>
                <urn4:LocalizedString value="XDSSubmissionSet.uniqueId"/>
            </urn4:Name>
        </urn4:ExternalIdentifier>
    </urn4:ExtrinsicObject>
    <urn4:RegistryPackage id="SubmissionSet01">
        <urn4:Slot name="esMDClaimId">
            <urn4:ValueList>
                <urn4:Value>1234567890123^^^&2.16.840.1.113883.13.34.110.1.999.1&ISO</urn4:Value
                >
            </urn4:ValueList>
        </urn4:Slot>
        <urn4:Slot name="esMDCaseld">
            <urn4:ValueList>
                <urn4:Value>12345678901234567890123456789001^^^&2.16.840.1.113883.13.34.110.1.999.1
                &ISO</urn4:Value>
            </urn4:ValueList>
        </urn4:Slot>
        <urn4:Slot name="intendedRecipient">
            <urn4:ValueList>
                <urn4:Value>2.16.840.1.113883.13.34.110.2.100.1</urn4:Value>
            </urn4:ValueList>
        </urn4:Slot>
        <urn4:Description>
            <urn4:LocalizedString value="esMD Claim Document Submission in response to
Review Contractor ADR Letter"/>
        </urn4:Description>
        <urn4:Classification id="cl11" classificationScheme="urn:uuid: a7058bb9-b4e4-4307-
ba5b-e3f0ab85e12d" classifiedObject=" SubmissionSet01" nodeRepresentation="author">

```

```

<urn4:Slot name="authorInstitution">
  <urn4:ValueList>
    <urn4:Value>897654</urn4:Value>
  </urn4:ValueList>
</urn4:Slot>
<urn4:Slot name="authorPerson">
  <urn4:ValueList>
    <urn4:Value>808</urn4:Value>
  </urn4:ValueList>
</urn4:Slot>
</urn4:Classification>
<urn4:Classification id="cl09" classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500" classifiedObject="SubmissionSet01"
nodeRepresentation="2.16.840.1.113883.13.34.110.1.1000.1">
  <urn4:Slot name="contentTypeCode">
    <urn4:ValueList>
      <urn4:Value>1</urn4:Value>
    </urn4:ValueList>
  </urn4:Slot>
  <urn4:Name>
    <urn4:LocalizedString value="Response to Additional Documentation Request
(ADR)"/>
  </urn4:Name>
</urn4:Classification>
<urn4:ExternalIdentifier id="ei03" registryObject="SubmissionSet01"
identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"
value="1234567890123^^^&2.16.840.1.113883.13.34&ISO">
  <urn4:Name>
    <urn4:LocalizedString value="XDSSubmissionSet.patientId"/>
  </urn4:Name>
</urn4:ExternalIdentifier>
<urn4:ExternalIdentifier id="ei04" registryObject="SubmissionSet01"
identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"
value="12.16.840.1.113883.13.34.110.2">

```

```

    <urn4:Name>
      <urn4:LocalizedString value="XDSSubmissionSet.sourceId"/>
    </urn4:Name>
  </urn4:ExternalIdentifier>
  <urn4:Slot name="submissionTime">
    <urn4:ValueList>
      <urn4:Value>20110101165910</urn4:Value>
    </urn4:ValueList>
  </urn4:Slot>
  <urn4:ExternalIdentifier id="ei05" registryObject="SubmissionSet01"
identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8" value="554ac39e-
ef6343434-b233-965d3434555">
    <urn4:Name>
      <urn4:LocalizedString value="XDSSubmissionSet.uniqueId"/>
    </urn4:Name>
  </urn4:ExternalIdentifier>
  <urn4:Name>
    <urn4:LocalizedString value="Claim Supporting Medical Documentation"/>
  </urn4:Name>
</urn4:RegistryPackage>
  <urn4:Classification id="cl10" classifiedObject="SubmissionSet01"
classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"/>
  <urn4:Association id="as01" associationType="HasMember"
sourceObject="SubmissionSet01" targetObject="Document01">
    <urn4:Slot name="SubmissionSetStatus">
      <urn4:ValueList>
        <urn4:Value>Original</urn4:Value>
      </urn4:ValueList>
    </urn4:Slot>
  </urn4:Association>
</urn4:RegistryObjectList>
</urn2:SubmitObjectsRequest>
<!--1 or more repetitions:-->

```

```
<urn5:Document id="Document01">[sample encrypted payload]</urn5:Document>  
</urn:ProvideAndRegisterDocumentSetRequest>  
</urn:RespondingGateway_ProvideAndRegisterDocumentSetRequest>  
</soapenv:Body>  
</soapenv:Envelope>
```

Appendix B. C62 Payload Sample

Note: The following CDA document will be sent in binary form with Base64 encoding. Here it is shown for information purposes only.

```
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" classCode="DOCCLIN" moodCode="EVN" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">
  <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
  <id root="eab8765b-1424-47cc-9495-ddc934cf5f5d"/>
  <templateId root="2.16.840.1.113883.10.20.3" assigningAuthorityName="CDT General Header
Constraints"/>
  <templateId root="1.3.6.1.4.1.19376.1.5.3.1.1.1" assigningAuthorityName="IHE Medical
Document"/>
  <templateId root="1.3.6.1.4.1.19376.1.2.20" assigningAuthorityName="IHE Scanned Document"/>
  <templateId root="2.16.840.1.113883.3.88.11.62.1" assigningAuthorityName="HITSP Unstructured
Document"/>
  <languageCommunication>
    <templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.1' />
    <languageCode code='en-US' />
  </languageCommunication>
  <title>ADR Response Supported Claim Documentation</title>
  <confidentialityCode code="V" codeSystem="2.16.840.1.113883.5.25"
codeSystemName="Confidentiality" displayName="Very Restricted"/>
  <effectiveTime value="20100319083838-0500"/>
  <recordTarget>
    <patientRole>
      <id extension="12345" root="2.16.840.1.113883.3.933"/>
      <addr>
        <streetAddressLine>NA</streetAddressLine>
        <city>NA</city>
        <state>NA</state>
        <postalCode>NA</postalCode>
        <country>NA</country>
      </addr>
      <patient>
        <name>
          <prefix>NA</prefix>
          <given>NA</given>
          <family>NA</family>
        </name>
        <administrativeGenderCode code="F"
```

```

      codeSystem="2.16.840.1.113883.5.1"/>
    <birthTime value="19600127"/>
  </patient>
</patientRole>
</recordTarget>
<author>
  <templateId root="1.3.6.1.4.1.19376.1.2.20.1"/>
  <time value="19990522"/>
  <assignedAuthor>
    <id extension="11111111" root="1.3.5.35.1.4436.7"/>
    <assignedPerson>
      <name>
        <prefix>NA</prefix>
        <given>NA</given>
        <family>NA</family>
        <suffix>NA</suffix>
      </name>
    </assignedPerson>
    <representedOrganization>
      <id extension="aaaaabbbb" root="1.3.5.35.1.4436.7"/>
      <name>NA</name>
    </representedOrganization>
  </assignedAuthor>
</author>
<author>
  <templateId root="1.3.6.1.4.1.19376.1.2.20.2"/>
  <time value="20050329224411+0500"/>
  <assignedAuthor>
    <id root="1.3.6.4.1.4.1.2835.2.1234"/>
    <assignedAuthoringDevice>
      <code code="CAPTURE" displayName="Image Capture" codeSystem="
1.2.840.10008.2.16.4" />
      <manufacturerModelName>NA</manufacturerModelName>
      <softwareName>NA</softwareName>
    </assignedAuthoringDevice>
    <representedOrganization>
      <id root="1.3.6.4.1.4.1.2835.2"/>
      <name>SOME Scanning Facility</name>
      <addr>
        <streetAddressLine>NA</streetAddressLine>
        <city>NA</city>
        <state>NA</state>
        <postalCode>NA</postalCode>
        <country>NA</country>
      </addr>
    </representedOrganization>
  </assignedAuthor>
</author>

```



```
</component>  
</ClinicalDocument>
```

Appendix C. Test Types for HIHs

This section provides descriptions and details for the five phases of testing that need to be performed by the HIHs during the testing of their gateways with the esMD Gateway. Successful completion of these tests is essential for the HIHs before they are declared production-ready.

The five phases of testing are as follows:

- Connectivity Test in Validation Environment (performed using SoapUI tool for the new HIHs and using the HIH gateway for onboarded HIHs).
- Functionality Test in Validation Environment (performed using the HIH application and HIH gateway and not through SoapUI tool).
- End-to-End Test in Validation Environment (performed using the HIH application and HIH gateway involving Review Contractor and not through SoapUI tool).
- Connectivity Test in Production Environment (performed using SoapUI tool for the new HIHs and the using HIH Gateway for onboarded HIHs).
- End-to-End Test in Production Environment (performed using the HIH application and HIH gateway involving Review Contractor and not through SoapUI tool).

The sections below explain the above tests in detail.

C.1 Connectivity Test in the Validation Environment

Tests are performed in this area to confirm connectivity between the HIH Gateway and the esMD Gateway. Confirmation of connectivity between the two gateways is essential before the esMD Gateway can receive and process the XDR deferred document submission requests sent from the HIH Gateway. New HIHs can use the SoapUI tool, if the HIH Gateway is not ready for this connectivity test. For details on how to configure SoapUI, please, refer to Appendix E.

C.2 Testing Inbound Connection (HIH Gateway to the esMD Gateway)

The purpose of this test is to ensure inbound connectivity between the HIH Gateway and the esMD Gateway using HIH IP Address validation at the CMS Verizon Router, CMS Firewalls, and TLS Mutual Certificate Authentication.

C.3 Inbound Telnet Test

The purpose of this sub-test is to verify whether the inbound network connection between the HIH Gateway and the esMD Gateway were established by doing the simple telnet test from the HIH Gateway. Under this test, the HIH IP addresses Inbound Configurations at the CMS Verizon Router/CMS Firewall will be verified.

Prerequisite:

- Participating HIHs will submit their public facing IP address to the esMD Team 7 weeks before the scheduled testing date. This is submitted via the HIH Introductory Details form.
Note: Any changes to the IP address after submission to the esMD Team could possibly cause a delay in testing and may result in the HIH being moved to the next onboarding group.
The HIH will verify with their firewall team whether their environment might need HIH outbound (HIH to the esMD Gateway) IP address NATing to the esMD Gateway. The esMD inbound IP address for 'esmdval.cms.hhs.gov' will be shared by the esMD HIH coordinators.
- The esMD Gateway Contractor, the CMS Hosting contractor, and Verizon teams will process and configure the HIH IP address routing rules in the CMS Verizon router and the CMS firewalls to allow the traffic from the HIH Gateway.

The following is a sequence of events at this level:

1. The esMD Team arranges a conference call with the HIH and the CMS Hosting contractor.
2. During the conference call, HIHs set up a telnet session between their gateway and the AT&T/CMS Firewall.
3. The CMS Hosting contractor watches over the incoming traffic from the HIH Gateway at the AT&T/CMS firewall level and confirms the inbound telnet connectivity.
4. HIH Gateway and Firewall teams will confirm the inbound telnet connectivity test at HIH end.

A successful telnet session indicates established inbound telnet connectivity between the HIH network and the CMS network.

C.4 HIH Mutual TLS Certificate Authentication

Based upon a successful Telnet session (Section C.3 Inbound Telnet Test), this step is performed during the same conference call, or a different conference call, depending upon the availability of resources from the esMD Team, the CMS Hosting contractor, and the HIH.

Prerequisite:

- Participating HIHs will submit their Gateway Certificate procured from Entrust CA Authority to the esMD Team 7 weeks before the scheduled testing date. *Any changes to the CA certificate after submission to the esMD Team could possibly cause a delay in testing and may result in the HIH being moved to the next onboarding group.
- The esMD Gateway Contractor, the CMS Hosting contractor, and Verizon teams configure the HIH IP address routing rules in the CMS Verizon router and the CMS firewalls to allow traffic from the HIH Gateway.
- HIH Gateway domain configuration will have the esMD specific TLS CIPHER Suites with FIPS Mode. The CMS CIPHER Suites will be added in the future.

The following are the sequence of events at this level:

1. The HIH submits the XDR deferred document submission request to the esMD Gateway.

2. The HIH TLS mutual Certificate authentication will occur between the HIH Gateway and the esMD environment in the following levels:
 - a. Mutual authentication between the CMS F5 Load Balancer appliance and the HIH Gateway;
 - b. TLS Cipher Suite validation between the CMS F5 Load Balancer appliance and the HIH Gateway; and
 - c. HIH Certificate validation at the esMD Gateway.
3. The successful mutual authentication between the HIH Gateway and the esMD Gateway will get an HTTP 200 Acknowledgment from the esMD Gateway to the HIH Gateway. The HIH will submit the test results to the esMD Team for confirmation.
4. The esMD Team and the CMS Hosting contractor will confirm the successful incoming mutual authentication.

C.5 Confirmation of Metadata Validation and Request Processing

The purpose of this step is to confirm successful metadata validation and request processing by the esMD Gateway. The esMD Team along with the CMS Hosting Contractor analyze the gateway and adaptor logs (along with database) to confirm metadata validation and request processing. If any anomalies are found, they are reported to the HIH.

C.6 Confirmation of Metadata Persistence in the esMD Database

In this step, the esMD DBA team analyzes the database for successful persistence of the audit events and data sent by the HIHs. All transaction related audit events and metadata persistence would be verified. Any errors or exceptions found are reported to the HIHs.

In addition, the esMD will send the errors and exceptions as a part of the esMD response message. These errors and exceptions can be found in the HIH the esMD Gateway logs.

C.7 Testing Outbound Connection (esMD Gateway to HIH Gateway)

The purpose of this test is to verify if the outbound connections are establishing between the esMD Gateway and the HIH Gateway.

C.8 Outbound Telnet Test

The purpose of this sub-test is to verify whether the outbound network connection between the HIH Gateway and the esMD Gateway were established by doing the simple telnet test from the esMD Gateway. Under this test, the HIH IP address outbound configurations at the CMS AT&T Router/CMS Firewall will be verified.

Prerequisite:

- Participating HIHs will configure their firewall to allow the esMD Gateway IP address prior to the scheduled testing date. The esMD Gateway outbound IP address will be shared by the esMD HIH coordinators.
- The HIH will verify with their firewall team if their gateway has the NATing for the inbound request coming from the esMD Gateway.

The following is a sequence of events at this level:

1. The esMD Team arranges a conference call with the HIH and the CMS Hosting contractor.
2. During the conference call, the esMD Team performs the telnet connection between the esMD Gateway and the HIH Gateway.
3. The HIH firewall team monitors the incoming traffic from the esMD Gateway at their firewall and confirms the outbound telnet connectivity.

A successful telnet session indicates established outbound telnet connectivity between the esMD Gateway and the HIH network.

This step is carried out in parallel to Section C.3 Inbound Telnet Test. A telnet session is set up to check the connectivity between the esMD Gateway and the HIH Gateway. A successful telnet session confirms connectivity between the two gateways.

C.9 Confirmation of Receiving the First Notification

Based on the results of the validations mentioned below, an asynchronous XDR Response message is sent to the HIH Gateway by the esMD Gateway:

- Validation of the syntax;
- Validation of the semantics with the esMD affinity domain values;
- Validation for duplicate Unique ID;
- Validation of the participation of intended recipient (i.e., the RC); and
- Validation of the HIH OID.

The response message could take anywhere from less than 1 minute up to 10 minutes based on the size of attachment (i.e., the payload). Confirmation of receipt of this notification message by the HIH indicates a success scenario.

Completion of all the above steps successfully confirms connectivity between the HIH Gateway and the esMD Gateway. A congratulatory email is sent by the esMD to the HIH indicating this success.

C.10 Functionality Testing in the Validation Environment (Testing with the HIH Gateway Application)

Tests in this phase are performed to confirm that the HIH application will send proper metadata and payload (PDFs) to the esMD Gateway, using their esMD application, and the esMD HIH Gateway. The esMD Gateway validates and processes the metadata and will deliver payload to the CMS Enterprise File Transfer system.

The purpose of this phase of testing is to test different functionality case scenarios to ensure the HIH Gateway is getting the proper acknowledgements, notifications, and error messages, if any, back from the esMD Gateway.

HIHs should refer to the test cases in Appendix C of this Guide, run the tests, and send the requests and response messages (i.e., results) to the esMD Team via the HIH coordinator. The esMD Team will analyze and report the results to the HIH.

C.11 Inbound Tests (HIH to the esMD Gateway)

The purpose of this test is to establish that the HIH Gateway is able to connect through their application and to verify that the HIH Gateway is able to establish the connection without using the SoapUI.

C.12 Validate Metadata and Request Processing

The XDR deferred document submission request is submitted by the HIH using its gateway application (and not SoapUI). The esMD Team analyzes the gateway and adaptor logs to confirm metadata validation and request processing. If any anomalies are found, they are reported to the HIH.

C.13 Metadata Persistence in the esMD Database

In this step, the esMD DBA team analyzes the database for successful persistence of the data sent by the HIHs. All transaction related audit events, submission related audit events, and metadata value persistence are checked for persistence. Any errors found are reported to the HIH.

C.14 Delivery to the CMS Enterprise File Transfer System

In this step, the esMD Team confirms the payload delivery to the CMS Enterprise File Transfer.

C.15 Outbound Tests (HIH to the esMD Gateway)

Delivery of the first notification response (about payload delivery to the CMS Enterprise File Transfer) to the HIH Gateway from the esMD Gateway confirms a successful scenario.

At the end of the Functionality Testing, a congratulatory email is sent by the esMD Team to the participating HIH.

C.16 End-to-End Testing in the Validation Environment (Testing with HIH Gateway Application and Not SOAP UI)

Tests in this phase are performed to ensure the HIH's submitted metadata is validated and delivered to the CMS Enterprise File Transfer and, ultimately, delivered on to the RC. In addition, this testing will ensure that once the RC picks up the submitted documents, the notification will be sent back to the HIH regarding the pickup status.

C.17 Testing with an Review Contractor

In advance of this step, the HIH is asked to send test submissions to RCs that they would normally do in PROD.. Any test PDF payloads can be used in this testing.

In this step, the HIH sends the XDR deferred document submission request, using their gateway application to the esMD Gateway.

The HIH coordinator facilitates communication with involved RCs to retrieve XML and PDF payloads. The HIH coordinator will record the results of testing and share with the HIH technical lead.

C.18 Receipt of Second Notification (Review Contractor Pickup)

After sending the XDR deferred document submission request to the esMD Gateway (step D.3.1.1 above), it is verified, if the HIH received the second notification from the esMD Gateway. Receipt of the second notification response (RC pick-up) confirms and concludes a successful end-to-end testing.

C.19 Connectivity Test in the Production Environment

The same steps outlined in Section C.3 Inbound Telnet Test are followed with this phase of testing in the PROD environment. The PROD DNS name after Release AR2016.03.01 is esmd.cms.hhs.gov.

C.20 End-to-End Testing in the Production Environment

The same steps outlined in Section C.16 End-to-End Testing in the Validation Environment (Testing with HIH Gateway Application and Not SOAP UI) are followed with this phase of testing in the Production environment.

Appendix D. SOAP UI Configuration

The purpose of this section is to provide the new HIHs with instructions for how to setup the SoapUI in their environment. The HIH must configure the SoapUI in order to use the SoapUI test cases provided by the esMD team. The SoapUI is necessary to allow the HIH to perform the connectivity testing. The HIH will submit the test through the SoapUI using their esMD Gateway establishing a connection to the esMD Gateway.

D.1 Download and Initial Configuration

1. Download and install SoapUI 3.5.1 from <http://sourceforge.net/projects/soapui/files/soapui/3.5.1>
2. After SoapUI has been installed, perform the following steps to complete the configuration:
 - a. Launch SoapUI;
 - b. Select the File -> Preferences option;
 - c. Make sure the HTTP version is set to 1.1;
 - d. Enter "300000" into the Socket Timeout field;
 - e. Press the "OK" button; and
 - f. Select the File -> Save Preferences menu option.
 - g. The Sample soap message is provided in the HIH Onboarding manual. If you are an authorized HIH and need the sample soap message, please contact the esMD Support team (esMD_Support@cms.hhs.gov).

D.2 Test Execution

The following steps outline the actions required to execute the Soap UI test.

1. Start Application Server on the Gateway machine and verify all desired applications are deployed.
2. Start the SoapUI application from the Soap UI Installation Directory.
3. Open the EndToEndSelfTest SoapUI project by selecting File->Import Project and navigate to the SoapUI Validation Suite Installation directory and select EndToEndSelfTest-soapui-project.xml.
4. Navigate to EndToEndSelfTest SoapUI project and change following custom properties before running the test:
 - a. LocalAA = HIH's OID
 - b. LocalHCID = HIH's OID
 - c. RemoteAA = CMS Val Gateway's OID
 - d. RemoteHCID = CMS Val Gateway's OID
5. Navigate to the EndToEndSelfTest TestSuite -> XDR Async -> Test Steps (1) -> EntityXDRRequest and double click it to open Soap message in XML Editor and change the Unique ID before running the test:

(i.e.,

<urn1:assertion>

<urn1:id>[UniqueID]</urn1:id>

.....

.....

</urn1:assertion>)

6. In the right panel (footer area) of the Soap UI tool, click on 'WS-A' button and change MessageID property before running the test:

Remember to change the UniqueID and Message ID before executing any test from the SoapUI tool.

Appendix E. Submission Guidelines for Certified HIHs

The esMD Gateway is built using the CONNECT software, which has a file size limitation of 200 MB per each submission. This file size of 200 MB includes the SOAP envelope packaging, the metadata, and the encoded PDF document. HIHs need to make sure the PDF payload should be **no more than 200 MB after encoding**.

With the implementation of the esMD Release AR2016.03.0 , submission requests with a payload size exceeding 200MB are rejected.

Appendix F. Submitting Transactions with CONNECT Version 3.1, or Older Versions

Note: Only CONNECT versions between CONNECT 3.1 and CONNECT 4.0 are supported. CONNECT 3.1 and previous versions are not supported.

If an HIH uses CONNECT 3.1 or previous versions, and sends an XDR payload with a file size of 0 MB, the HIH will still receive an HTTP 200 Acknowledgement that there was a successful transfer of the XDR payload to the esMD's gateway; however, the esMD system will not generate or send an error message that an XDR payload with a file size of 0 MB was transferred to the esMD gateway.

A Transaction ID will not be assigned to an empty payload (a payload with a file size of 0 MB) transaction and no further processing of the empty payload transaction will take place. This will only happen when CONNECT 3.1 or previous versions, after the rollout of the esMD Release 4.0 system.

Note: The CGI CONNECT Team will no longer provide support for CONNECT 3.1, or any other CONNECT version older than CONNECT 3.1.

The CGI CONNECT Team suggests that all end users upgrade to CONNECT Release v4.4.

The esMD system is using CONNECT Release v4.4.

After upgrading to CONNECT Release v4.4, the esMD Support Team will no longer be able to provide support for CONNECT 3.1 or previous versions. The esMD Support Team will not be able to provide support for CONNECT versions that are no longer being supported by the vendor.

HIHs that upgrade will continue to receive support from both the esMD Support Team and the CGI CONNECT Team.

When the esMD Support Team looks into an inquiry about a transaction and discovers there is a transaction with an empty payload (a payload with a file size of 0 MB), the esMD Support Team will inform the HIH that the esMD system has received an empty payload, a Transaction ID has not been assigned to the transaction, and the HIH will need to resend the transaction with the correct payload attached.

Appendix G. PA Reason Identifiers and Statements

The Reason Identifiers for the PA Responses can be found online in the following file on the CMS website: <https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/CERT/Downloads/PMD-PA-Demo-Reason-Identifiers-and-Statements-June-2013.pdf>

Appendix H. References

- HL7 CDA Release 2
 - Org/SDO: Health Level 7
 - Version: 3
 - Link:
This information may be found in the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- HL7 Implementation Guide for CDA[®] Release 2: IHE Health Story Consolidation, Release 1.1 - US Realm
 - Org/SDO: Health Level 7
 - Version: 3
 - Link:
This information may be found in the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- NHIN Exchange Service Interface Specification CAQH CORE X12 Document Submission Service Interface Specifications
 - Org/SDO: eHealth Exchange
 - Version: 1.0
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- NHIN Exchange Messaging Platform Specification
 - Org/SDO: eHealth Exchange
 - Version: 3.0
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- NHIN Exchange Authorization Framework Specification
 - Org/SDO: eHealth Exchange
 - Version: 3.0
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:

- https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
- NHIN Exchange Document Submission Production Web Service Interface Specification
 - Org/SDO: eHealth Exchange
 - Version: 2.0
 -
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
- NHIN esMD XDR Production Specification
 - Org/SDO: eHealth Exchange
 - Version: 1.0
 - Link:
http://exchange-specifications.wikispaces.com/file/view/THE_ESMD_XDR_Production_Specification_v1.0.pdf
- CAQH Phase II CORE 270 Connectivity Rule
 - Org/SDO: CAQH CORE
 - Version: 2.2.0
 - Link:
<http://www.caqh.org/core/caqh-core-phase-ii-rules>
- XDR and XDM for Direct Messaging Specification
 - Org/SDO: DirectTrust.org
 - Version: 1.0
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
- IHE XDR Cross-Enterprise Document Reliable Interchange (XDR)
 - Org/SDO: IHE
 - Version: 9.0
 - For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
- IHE XDS Provide and Register Document Set-b IHE IT Infrastructure 5 Technical Framework Volume 2b (ITI TF-2b) Transactions Part B
 - Org/SDO: IHE
 - Version: 9.0

- For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- For ASC X12N 278 information, see ASC X12
 - Org/SDO: ASC X12
 - Version: 5010
 - Link:
<http://store.x12.org/store/>

- ASC X12N TA1
 - Org/SDO: ASC X12
 - Version: 5010
 - Link:
<http://store.x12.org/store/healthcare-5010-original-guides>

- ASC X12N 999
 - Org/SDO: ASC X12
 - Version: 5010
 - Link:
<http://store.x12.org/store/healthcare-5010-original-guides>

- Electronic Determination of Coverage: Implementation Guide with ASC X12N 278 Transaction Sets
 - Org/SDO: Standards & Interoperability Framework
 - Version: V24
 - Link:
<http://wiki.siframework.org/file/view/esMD%20eDoC%20Implementation%20Guide%20278%20V24.docx/514433788/esMD%20eDoC%20Implementation%20Guide%20278%20V24.docx>

- Approved esMD External Data Representation (XDR) Profile Definition Version 1.0, refer to:
 - http://wiki.siframework.org/file/detail/ESMD+Profile+v11.1_02162011_XDR_Draft_Final_dj.doc

- Integrating the Healthcare Enterprise (IHE) Deferred Cross-Enterprise Document Reliable Messaging (XDR) (refer to v1.1.0.6).

- For more information on this, please refer to the "Related Documents" or "Implementation Guide" sections on the following web site:
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

- Trial Implementations Document Submission Interface Specification Version 1.1.0, refer to:
http://exchange-specifications.wikispaces.com/file/view/ESMD_XDR_Production_Specification_v1.0.pdf

- Trial Implementations Message Platform Service Interface Specification Version 3.0, refer to:
<http://www.healthit.gov/sites/default/files/nhin-messaging-platform-production-specification-v3.0.pdf>

- Authorization Framework Specification Version 2.0 refer to
<http://www.healthit.gov/sites/default/files/nhin-authorization-framework-production-specification-v2.0-1.pdf>

- IHE TF3 Cross-Transaction Specifications and Content Specifications Version 6.0 refer to
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_6-0_Vol3_FT_2009-08-10-2.pdf

Appendix I. The esMD Sample CAQH Real-Time Request

```
<urn:RespondingGateway_CrossGatewayRealTimeRequest>
  <cor:COREEnvelopeRealTimeRequest>
    <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
    <ProcessingMode>RealTime</ProcessingMode>
    <PayloadID>f81d4fae-7dec-11d0-a765-00ash</PayloadID>
    <TimeStamp>2014-12-19T10:20:34Z</TimeStamp>
    <SenderID>urn:oid:123.456.657.132</SenderID>
    <ReceiverID>urn:oid:2.16.840.1.113883.13.34.110.1.999.1</ReceiverID>
    <CORERuleVersion>v2.2.0</CORERuleVersion>
    <Payload>ISA*00*      *00*      *ZZ*9012345720000 *ZZ*9088877320000
*081208*0817*+*00501*000001523*0*T*;!
GS*HI*901234572000*908887732000*20081208*1615*1523*X*005010X217!
ST*278*1523*005010X217!
BHT*0007*01*3920394930203*20081208*1615*RU!
HL*1**20*1!
NM1*X3*2*JOHNSON*****46*2.16.840.1.113883.13.34.110.1.999.1!
HL*2*1*21*1!
NM1*1P*1*SMITH*MUFFY*M**PH.D*XX*111111112!
N3*PO BOX 123!
N4*CINCINNATI*OH*43017!
PER*IC*WILBER*FX*8189991234*TE*8187691304*EX*5189657704!
PRV*CO*PXC*208D00000X!
HL*3*2*22*1!
NM1*IL*1*JONES*BARBARA*T*MR*M.D.*II*AA123456!
N3*PO BOX*123!
N4*CINCINNATI*OH*43017!
DMG*D8*19511204*F!
HL*4*3*EV*0!
TRN*1*12345678900987654321768958473*1311234567*500!
```

UM*IN*I*1*13:A*AA:EM:AP:ON:CA*U*3*4*Y*1!
NM1*72*1*JOHNSON*BARBARA****46*111111111!
N3*PO BOX 123!
N4*CINCINNATI*OH*43017!
SE*22*1523!
GE*1*1523!
IEA*1*000001523!</Payload>
</cor:COREEnvelopeRealTimeRequest>

Notes:

- 1) NM1 2010 segment should not include urn:oid qualifier for the Receiver ID;
- 2) Sender ID in the ISA segment must be the EDI ID (15 alphanumeric) that was provided by the HIH during the HIH onboarding process; and
- 3) Receiver ID in the ISA segment must be the Review Contractor ID (15 alphanumeric) that was provided by the RC during the RC onboarding process.