



Nationwide Health Information Network (NHIN)

Electronic Submission of Medical Documentation (esMD)

esMD XDR Production Specification



V 1.0

06/27/2011



Contributors

Name	NHIO Represented	Organization
Dan Kalwa	CMS	CMS
Melanie Combs-Dyer	CMS	CMS
Aaron Walton	CMS	Edaptive
Craig Miller	ONC	Vangent
Manoj Chaganti	CMS	QSSI
Karen Witting	IBM	IBM
Sacchidanand Girde	CMS	QSSI
Donna Jones	CMS	Signature Consulting

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
0.0.1		Melanie Combs-Dyer	Initial Draft
0.0.2		Aaron Walton, Edaptive Systems	Revised draft – removed all references to C163 and 275 formats
0.0.3		Aaron Walton, Edaptive Systems	Revised draft – added sections 2 and 3
0.0.4		Aaron Walton, Edaptive Systems	Revised draft – added error message table and URN specifications
0.0.5		Daniel Kalwa, CMS	Revised Draft – Rearranged error messaging section, moved all submission specifications to correct section.
0.0.6	5/12/10	Aaron Walton, Edaptive Systems	Incorporated CMS requested format changes.
0.0.7	5/12/10	Daniel Kalwa, CMS	Revised Draft – Edited sections with legacy PQRI statements.
0.0.8	5/17/10	Daniel Kalwa, CMS	Revised Draft – Edited sections with legacy PQRI statements. Updated section with Keith Boone's suggested language.
0.0.9	5/18/10	Jackie Key	Updated version # to reflect finalization of draft profile, contributors table, adjusted formatting, and moved content from introduction to assumptions section
0.1	01/09/2011	Manoj Chaganti	Reviewed and revised all the sections of this draft Section 1.1 – added CERT and PERM details. Section 1.2 – updated Intended Audience Content Section 1.3 – updated Business needs and its content. Section 1.4 – Added references to Authentication (SAML), XDR and security specifications. Section 2.0 – Updated Profile definition content. Section 2.1 – Updated Design Principals and assumptions. Section 3. – Added NHIN exchange of esMD Data details and its SOAP envelope diagram. Section 3.1 – Added SAML Authentication details Section 3.2 – Added Submission Set and Document Metadata Section 3.3 – Added esMD extra Metadata attributes or XDR Slots Section 4.0 – Added Acknowledgment and responses Section 5.0 – Added Error Handling Error messages Section 6.0 – Updated the C62 Content overview Section 7.0 – Added esMD Glossary.
0.11	03/2/2011	Karen Writing	Updated and reviewed – Metadata details.
0.12	03/04/2011	Manoj Chaganti	Updated and reviewed – Metadata details and NHIN was added
0.13	03/21/2011	Manoj Chaganti/Karen	Updated and reviewed – Reviewed the content and updated the various sentences.



Electronic Submission of Medical Documentation (esMD)
Production Specification v1.0



0.14	04/12/2011	Manoj Chaganti/Karen	Updated and reviewed – SAML and Metadata details.
0.14	04/12/2011	Manoj Chaganti/Karen/S. Girde	Updated and reviewed – Metadata details were cleaned up and reviewed with NHIN Spec factory.
0.15	04/25/2011	Manoj Chaganti/Karen	Updated and reviewed – Karen comments were addressed in various sections of this document related to Document Submission Set.
0.16	05/16/2011	Manoj Chaganti	Updated and reviewed – SAML/Metadata/Diagrams/Document Submission Deferred Request/Response. TIFF format references were removed.
0.17	6/02/2011	Donna Jones	Revised Draft: - Spec Factory <ul style="list-style-type: none"> • Changed Profile to Specification • Changed NwHIN to NHIN • Changed purpose for use to purpose of use • Changed document submission version in section 3.2 from 1.1 to 2.0
0.18	6/08/2011	Donna Jones/S. Girde/Manoj Chaganti	Revised Draft: <ul style="list-style-type: none"> • Added lines numbers • Fixed spelling error on pg 11 • Sec 3.1 - Changed name to Authorization Framework • Went through to omit TIFF and only have PDF • Changed version # and link for Document Submission Spec in Section 1.4 on Page 6 • Removed TIFF reference from SOAP Message Format diagram on Page 10 • Updated section 4 on Pages 16, 17 & 18 to reflect changes mentioned in the Document Submission Production Web Service Interface Specification v 2.0 • Removed TIFF image resolution reference from Section 6.2 on page 21 • Reviewed wording in the entire document • Corrected the header from profile to specification • Sec. 1.4, #4 changed version from 2.0/2.2 to 2.0 • Added reference to NHIN Messaging Platform Specification v2.0 in Section 1.4
1.0	6/27/2011	ONC	Finalized for Production Publication

Document Approval

Version	Date	Approved By	Role
0.18	6/27/2011	NHIN Technical Committee	Approves all specifications for production NHIN use



Table of Contents

1	PREFACE	4
1.1	INTRODUCTION	4
1.2	INTENDED AUDIENCE	4
1.3	BUSINESS NEEDS SUPPORTED.....	5
1.4	REFERENCED DOCUMENTS AND STANDARDS	5
1.5	RELATIONSHIP TO OTHER NHIN SPECIFICATIONS	8
2	PROFILE DEFINITION	8
2.1	DESIGN PRINCIPLES AND ASSUMPTIONS	9
2.2	TECHNICAL PRE-CONDITIONS	9
2.3	TECHNICAL POST-CONDITIONS	9
3	NHIN EXCHANGE OF ESMD DATA.....	10
3.1	AUTHENTICATION FRAMEWORK.....	10
3.2	SUBMISSION SPECIFICATIONS	11
3.3	EXTRA METADATA ELEMENTS	16
4	ACKNOWLEDGMENT AND RESPONSES (STATUS AND NOTIFICATION MESSAGES)	17
5	ERROR HANDLING	19
6	ESMD C62 CONTEXT OVERVIEW.....	19
6.1	SUBMISSION SPECIFICATIONS	21
6.2	ATTACHMENTS IN THE ESMD C62 FORMAT	22
7	GLOSSARY	23
8	ACRONYMS.....	25



1 1 Preface

2 1.1 Introduction

3
4 For 2009 the Medicare fee-for-service (FFS) program made an estimated \$34.3 billion in improper
5 payments. The Medicaid program made an estimated \$22.5 billion in improper payments. Medicare
6 review contractors compare the claims submitted by Medicare providers against entries in medical
7 records to measure, prevent, and correct improper payments.

- 8
9 • **RACs identify and correct improper payments.** Recovery Audit Contractors (RACs) conduct
10 post-payment review by comparing information from medical records to Medicare claims. The
11 Centers for Medicaid & Medicare Services (CMS) estimates that RACs will request over 1 million
12 medical records from providers each year.
- 13
14 • **MACs prevent improper payments.** Medicare Administrative Contractors (MACs) conduct pre-
15 payment and post-payment reviews of Medicare FFS claims. CMS estimates that MACs will
16 request several thousand medical records per year.
- 17
18 • **CERT and PERM contractors measure improper payments.** The Comprehensive Error Rate
19 Testing (CERT) contractor measures improper payments in the Medicare program. The Program
20 Error Rate Measurement (PERM) contractor measures improper payments in the Medicaid
21 program. CERT and PERM request thousands of medical records each year.
- 22

23 Prior to the Electronic Submission of Medical Documentation (esMD) Phase 1 pilot, the provider had
24 three choices when responding to these documentation requests: mail paper, mail a CD containing a
25 Portable Document Format (PDF) file, or transmit a fax. The esMD pilot will give providers an additional
26 option for responding to these requests for medical documentation: electronic transmission via the
27 Nationwide Health Information Network (NHIN).

28
29
30 1.2 Intended Audience

31 The primary audiences for this document include:

- 32 • Medicare Review Contractors that will receive medical documentation in esMD format sent by
33 Health Information Handlers on behalf of Medicare providers,
- 34 • Developers of software that aim to assist Medicare Review Contractors in viewing and more
35 efficiently processing documents received in esMD format,
- 36 • Health Information Handlers that will send medical documentation in esMD format to the
37 Medicare Review Contractors on behalf of Medicare providers,
- 38 • Developers of Electronic Health Records (EHR) extraction software that assist Health Information
39 Handlers more easily extract data from EHRs into the esMD format.

40 It is assumed that the readers have prior knowledge of IHE XDR Cross-Enterprise Document Reliable
41 Interchange (XDR), which provides a standards-based specification for managing the interchange of
42 documents that healthcare enterprises have decided to explicitly exchange using a reliable point-to-point
43 network communication and Health Information Technology Standards Panel (HITSP) C62 Unstructured



44 Document Component, which provided for the capture and storage of patient identifiable, unstructured
45 document content, such as PDF, and images rendered in PDF format.

46

47 1.3 Business Needs Supported

48

49 The esMD Phase 1 pilot will support the submission of documentation by providers such as physicians
50 and hospitals to a limited number of Medicare Review Contractors.

51 The purpose of this profile is to describe the esMD XDR communication interchange with HITSP C62
52 payload formats and provide background information about the underlying standards upon which the
53 esMD document submission messages are based. It is intended to:

- 54 • Communicate the data requirements necessary for Electronic Health Record (EHR) vendors to
55 incorporate into the design and development of their EHR products, and
- 56 • Serve as the roadmap for Health Information Handlers (HIHs) such as Regional Health
57 Information Organizations (RHIOs), Health Information Exchanges (HIEs), Release of
58 Information (ROI) vendors, and claim clearinghouses to use on behalf of providers submitting
59 documentation to Medicare Review Contractors.

NOTE: This document will refer to RHIOs, HIEs, ROI vendors, claim clearinghouses and
others entities that move health information over NHIN gateways on behalf of health care
providers known as "Health Information Handlers."

60 Only a limited number of HIHs will be selected to participate in the esMD Phase 1 Pilot.

61 This esMD XDR profile describes the **content** rules (e.g., what goes in which fields) and **submission**
62 rules (e.g., how to address the packages,) for the esMD pilot. CMS will develop a different document
63 called an "esMD Implementation Guide" to provide more implementation details such as onboarding
64 process, CMS esMD affinity values, Review Contractor numbers, etc.

65 1.4 Referenced Documents and Standards

66 The following documents and standards were referenced during the development of this profile. Specific
67 deviations from, or constraints upon, these standards are identified below.

68 1) **Org/SDO name:** HITSP

69 **Reference # / Spec Name:** C62 Unstructured Document Component

70 **Version #:** v.1.1

71 **NHIN Deviations or Constraints:** None

72 **Underlying Specs:** None

73 **Link:**

74 <http://wiki.hitsp.org/docs/C62/C62-1.html>

75

76 2) **Org/SDO name:** Centers for Medicare & Medicaid Services

77 **Reference # / Spec Name:** esMD XDR Implementation Guide

78 **Version #:** v.1.0



- 79 **NHIN Deviations or Constraints:** **None**
- 80 **Underlying Specs:** **None**
- 81 **Link:** <http://nhin-exchange.wikispaces.com/CMS+esMD>
- 82 At the time this document was published, the esMD Implementation Guide was not yet published
83 by CMS. This document will be updated once the Implementation Guide is available.
- 84
- 85 **3) Org/SDO name:** NHIN
- 86 **Reference # / Spec Name:** Document Submission Production Web Service Interface
87 Specification
- 88 **Version #:** v.2.0
- 89 **NHIN Deviations or Constraints:**
- 90
 - 91 • Deviation from XDS Metadata defined within IHE ITI TF-3 Rev. 6.0 as described in
92 section 3.2 "Submission Specifications"
- 93 **Underlying Specs:** IHE Cross-Enterprise Document Reliable Interchange
- 94 **Link:**
- 95 http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5158_1407_16910_43/http%3B/wc
96 [i-](http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5158_1407_16910_43/http%3B/wc)
97 [pubcontent/publish/onc/public_communities/k_o/nhin/resources/resources_home_portlet/files/nhi](http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5158_1407_16910_43/http%3B/wc)
98 [n_document_submission_production_specification_v2_0.pdf](http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5158_1407_16910_43/http%3B/wc)
- 99 **4) Org/SDO name:** NHIN
- 100 **Reference # / Spec Name:** NHIN Authorization Framework Specification
- 101 **Version #:** v.2.0
- 102 **NHIN Deviations or Constraints:** None
- 103 **Underlying Specs:** NHIN Authorization Framework Specification 2_0
- 104 **Link:**
- 105 http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910545_0_0_18/NHIN_Autho
106 [rizationFrameworkProductionSpecification_v2.0.pdf](http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910545_0_0_18/NHIN_Autho)
- 107
- 108 **5) Org/SDO name:** NIST/FEDERAL INFORMATION PROCESSING STANDARDS (FIPS 140-2)
- 109 **Reference # / Spec Name:** Security Requirements for CRYPTOGRAPHIC Modules
- 110 **Version #:** FIPS PUB 140-2
- 111 **NHIN Deviations or Constraints:** This standard specifies the security requirements that will be
112 satisfied by a cryptographic module utilized within a security system protecting sensitive, but
113 unclassified, information (hereafter referred to as sensitive information). The standard provides
114 four increasing, qualitative levels of security: Level 1 and Level 2. These levels are intended to
115 cover the wide range of potential applications and environments in which cryptographic modules
116 may be employed. The security requirements cover areas related to the secure design and
117 implementation of a cryptographic module. These areas include cryptographic module
118 specification, cryptographic module ports and interfaces; roles, services, and authentication, finite



119 state model; physical security; operational environment; cryptographic key management;
120 electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design
121 assurance; and mitigation of other attacks. This standard supersedes FIPS 140-1, Security
122 Requirements for Cryptographic Modules, in its entirety. The Cryptographic Module Validation
123 Program (CMVP) validates cryptographic modules to Federal Information Processing Standard
124 (FIPS) 140-2 and other cryptography based standards. Products validated as conforming to FIPS
125 140-2 are accepted by the CMS for the protection of sensitive information. The goal of the CMVP
126 is to promote the use of validated cryptographic modules and provide Federal agencies with a
127 security metric to use in procuring equipment containing validated cryptographic modules.

128
129 **Underlying Specs:** None

130 **Link:** <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

131
132 6) **Org/SDO name:** CMS / CMS Information Security ARS - CMSR Moderate Impact Level Data
133 **Reference # / Spec Name:** Appendix B - CMSR Moderate Impact Level Data
134 **Version #:** CMS-CIO-STD-SEC01-1.0
135 **NHIN Deviations or Constraints:** All cryptographic modules used by an HIH must adhere to
136 FIPS 140-2 Compliance criteria and utilize TLS. The FIPS 140-2 is a CMS standard that provides
137 a benchmark for implementing the cryptographic module.
138

139 **Underlying Specs:** <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

140 **Link:** http://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf

141
142 7) **Org/SDO name:** NHIN
143 **Reference # / Spec Name:** NHIN Messaging Platform Specification
144 **Version #:** v.2.0
145 **NHIN Deviations or Constraints:** None

146 **Underlying Specs:** None

147 **Link:**
148
149 [http://healthit.hhs.gov/portal/server.pt/document/910523/nhin_messagingplatformproductionspecif
150 ication_v2_0_pdf](http://healthit.hhs.gov/portal/server.pt/document/910523/nhin_messagingplatformproductionspecification_v2_0_pdf)
151
152
153

154



155

1.5 Relationship to other NHIN Specifications

157 This profile is related to other NHIN specifications as described below:

- 158 • **Messaging Platform** – specifies a base set of messaging standards and web service protocols
159 which must be implemented by each NHIN node and applies to all transactions. All NHIN inter-
160 nodal messages are Simple Object Access Protocol (SOAP) messages over Hypertext Transfer
161 Protocol (HTTP) using web services, and must be encrypted and digitally signed.
- 162 • **Authorization Framework** – defines the exchange of metadata used to characterize each NHIN
163 request. The purpose of that exchange is to provide the responder with the information needed
164 to make an authorization decision for the requested function. Each initiating message must
165 convey information regarding end user attributes and authentication using Security Assertion
166 Markup Language (SAML) 2.0 assertions.
- 167 • **Document Submission** – allows an initiating HIH NHIE node to “push” one or more Medicare
168 claim related patient-centric documents to CMS esMD NHIE node.

169 Together, the Messaging Platform and the Authorization Framework define the foundational messaging,
170 security and privacy mechanisms for the NHIN.

171

2 Profile Definition

172

173 This profile defines how esMD program data may be submitted by healthcare providers to the U.S. CMS
174 using the NHIN. The profile also describes the asynchronous multi-acknowledgement/response feedback
175 using the NHIN deferred messaging workflow pertaining to these submissions which may be sent by CMS
176 to healthcare providers.
177

178 The approach taken in the development of this specification was to balance the needs of:

- 179 • Medicare Review Contractors that desire to receive all data in an unstructured and structured
180 payload format to facilitate the review of Medicare claims, and
- 181 • Many HIHs that still retain some patient records in an unstructured format (such as imaged PDF
182 files).

183 As a result of this balanced approach, the esMD Phase I pilot will accept medical documentation only in
184 the following payload format:

Name of Specification	Purpose	Structured or Unstructured	What Section in this Document
HITSP C62	For submitting any type of documentation in PDF format	Unstructured	Section 3

185

186 The U.S. HITSP identified Health Level 7 (HL7) CDA R2 as the exchange standard for the electronic
187 movement of health-related information among organizations according to nationally recognized
188 standards. The CDA documents are well-known to the EHR vendors, and there is an existing certification
189 process by Certification Commission for Healthcare Information Technology (CCHIT) for generation and
190 consumption of CDA documents by EHR systems.

191



192 **2.1 Design Principles and Assumptions**

193 The following assumptions or design principles underlie this profile:

- 194 • **The provider decides what to submit.** In both the current paper process and the new esMD
195 process, the Medicare Review Contractor does not specify what the provider must send. It is up
196 to the provider to decide which documents to send. This often includes discharge summaries,
197 progress notes, orders, radiology reports, lab results, etc.
- 198 • **The esMD Phase I pilot will allow providers to submit only unstructured documents**
199 (imaged documents in PDF format).
- 200 • **The esMD future phases will allow providers to submit both unstructured and structured**
201 **documents.** The provider will have the option of sending structured documents or unstructured
202 documents. Submission of structured documents will be addressed in future esMD profiles.
- 203 • **One Way Transmission: Provider-to-Review Contractor.** The esMD Phase I pilot will be
204 unidirectional (provider-to-Medicare Review
205 Contractor). Future phases will allow the Medicare
206 Review Contractor to send the documentation request
207 letter to the provider electronically.
- 208 • **Each package must contain documentation about a**
209 **single Medicare beneficiary.** Throughout this profile,
210 the term “package” will be used to refer to one or more
211 Medicare claim supporting documents associated with
212 a single Medicare claim. Each package can contain
213 multiple Medicare claim supporting documents,
214 provided all documents are related to the same Medicare claim. This package is carried via a
215 single SOAP message.

The esMD Phase I pilot will allow providers to respond to RAC and MAC documentation requests via the Nationwide Health Information Network (NHIN).

216
217 **2.2 Technical Pre-conditions**

218 No technical pre-conditions have been identified specifically for this profile beyond those given in
219 referenced specifications.

220 **2.3 Technical Post-conditions**

221 No technical post-conditions have been identified specifically for this profile beyond those given in
222 referenced specifications.

223
224

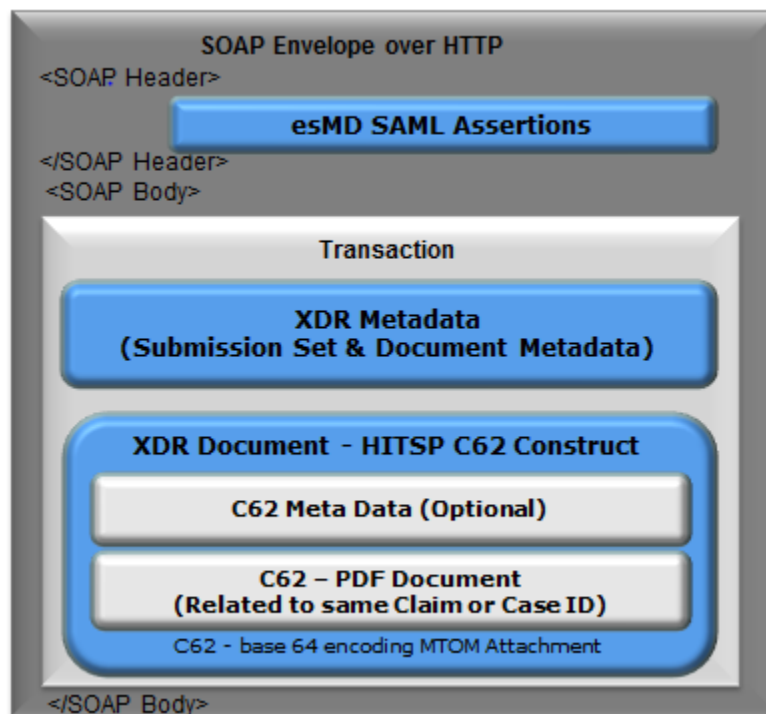
225 **3 NHIN Exchange of esMD Data**

226 This profile utilizes the NHIN Document Submission service interface specifications with SOAP envelope
227 messages under web service interfaces. HIH NHIE and CMS esMD communication would be as follows:
228 HIH Sends the SOAP Messages to CMS with SAML Assertions, Submission Set and Payload Meta Data
229 and reference to base 64 encoded MTOM C62 attachments in SOAP Body.

230

231

Figure: SOAP Message Format



232

233

234 **3.1 Authorization Framework**

235 esMD will follow the NHIN Authorization Framework with SAML assertions.

236

237 Normative: Implementers of the esMD Profile MUST implement security, transport, and messaging as
238 specified in the current versions of the NHIN Exchange Authorization Framework and Messaging Platform
239 specifications. Implementations MUST use FIPS Level 2 assurance or TLS.

240

241 Non-normative: CMS imposes Level 2 or greater FIPS assurance levels constraints.

242

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

249



- 250 • SAML Assertions would contain the HIH Organization Identification (OID) and Community
251 Identification (OID), Provider Identification (NPI) and Intended Recipient.
252 • Authentication
253 o Exchange 2Way TLS – Mutual authentication of the certs
254 o OID verification against CMS certified HIH based on CMS onboarding Process
255 o Document Hashcode verification with base 64 encoding - MD5
256 o FIPS 140-2 / Moderate Level Security
257
258

259 esMD XDR authentication will be implemented with the SAML assertions and 2 way TLS. Following are
260 the esMD specific SAML assertions attributes.
261
262

Table with 3 columns: S.No, SAML assertion Attribute, R/ R2/ O. Row 1: 1, IntendedRecipient, R

263 The purpose of use for all submissions shall be labeled as "Payment".
264
265

266 Assertions Standards are
267

- 268 • NHIN Authorization Framework v 2.0
269 • OASIS Security Assertion Markup Language (SAML) V2.0,
270 • Authentication Context for SAML V2.0,
271 • Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML for Healthcare
272 Version 1.0 OASIS Web Services Security: SAML Token Profile 1.1 specifications.
273

274 3.2 Submission Specifications
275

276 esMD will follow and adopt the IHE Cross Enterprise Document Reliable Interchange (XDR) profile in
277 SOAP Envelope with XDS Repository Submission Request Provide and Register Document set – b (ITI-
278 41) transaction metadata and C62 document payload with MTOM, base 64 encoded attachments.
279

280 esMD Document submission specifications shall conform with Nationwide Health Information Network
281 (NHIN Document Submission v2.0) transmissions.
282

283 The XDR XML body element will contain a reference to the attached Medicare claim document/s, where
284 the metadata information block is encapsulated with the XDR submission set and its document attributes.

285 All the unstructured document/s will be embedded in the HITSP C62 construct in PDF format.
286

287 In the initial implementation, submitters and responders shall always use a C62 payload as defined by
288 HITSP to carry unstructured data (UTF8 such as PDF as described in the first paragraph). In later
289 implementations, submitters and responders will be able to use structured and unstructured payload data.
290
291
292
293
294
295



296
297

Table: XDR Submission Set Metadata Attributes

S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2 /O
1	Extension	urn:nhin:esMD:ClaimId	Claim Identifier is the identifier, with which the provider submits the Claim to CMS. This could be found in the Additional Documentation Request (ADR) letter from Review Contractor.	R
2	Extension	urn:nhin:esMD:Caseld	Case Identifier is the identifier, generated by the Review Contractor to open a claim specific case. This could be found in Additional Documentation Request (ADR) letter from the Review Contractor if the request is from MACs.	R2
3	Existing	IntendedRecipient	Intended Recipient represents the organization(s) or person(s) for whom the Document Submission set is intended. In esMD, the Intended Recipient will be an organization (Review Contractor) to whom the sender (HIH) will submit the message with esMD Claim supporting Documents. This Intended Recipient will be identified by an HL7 issued organizational identifier (OID).	R
4	Existing	author	Represents the provider (NPI), who submits the Claim Supporting Documents in response to the Additional Documentation Request letter (ADR) from the CMS Review Contractor This attribute could contain the following sub-attributes based on who (either Provider or institution NPI) submits the documentation: authorInstitution authorPerson	R
4.1	Existing	authorInstitution (sub-attribute of author)	If there is only one document in the SubmissionSet, authorInstitution attribute of the SubmissionSet shall have the same NPI as the one used in the authorInstitution attribute at the document level. If there is more than one document in the SubmissionSet, authorInstitution attribute of the SubmissionSet shall have the NPI of the organization/institution which put together all the documents included in the SubmissionSet.	R2



S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2 /O
			Please note: At the SubmissionSet level either the authorInstitution or authorPerson attribute shall be used but never both.	
4.2	Existing	authorPerson (sub-attribute of author)	<p>If there is only one document in the SubmissionSet, authorPerson attribute of the SubmissionSet shall 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 shall have the NPI of the provider who put together all the documents in the SubmissionSet.</p> <p>Please note: At the SubmissionSet level either the authorInstitution or authorPerson attribute shall be used but never both.</p>	R2
5	Existing	comments	Comments associated with the SubmissionSet in a free form text format	O
6	Existing	contentTypeCode	The submission set is a response to Additional Documentation Request (ADR) from the Review Contractor. The ContentTypeCode is the code that specifies this – a Response to ADR.	R
7	Existing	entryUUID	<p>A unique ID or a globally unique identifier within the document submission request for the SubmissionSet.</p> <p>For example, “SubmissionSet01” can be <i>entryUUID</i>. It can also be in the UUID format.</p>	R
8	Existing	patientId	<p>This is a required XDR field. Since esMD is Claim centric (and not Patient centric), esMD shall populate this field with Claim ID using the format: ‘Root + Extension’. esMD shall use CMS OID as the root and Claim ID as the extension, like so:</p> <p>CMS OID.esMDClaimID</p> <p>It is important to remember that Claim ID will also be populated in the attribute ‘urn:nhin:esMD:ClaimId’ mentioned in row 1 of this table in addition to being populated here.</p>	R
9	Existing	sourceId	Globally unique identifier, in OID format, identifying the Health Information Handler (HIH) Gateway through which document/s were sent to the CMS esMD Gateway.	R
10	Existing	submissionTime	Point in Time when the SubmissionSet	R



S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2 /O
			was created at the HIH CONNECT Adapter level	
11	Existing	title	Represents the title of the Submission Set. esMD Title for the Document submissionSet shall be – ‘Claim Supporting Medical Documentation’.	O
12	Existing	uniqueId	A globally unique identifier, in OID format, assigned by the HIH to the submission set in the transmission. The length of this Unique Identifier shall not exceed 128 bytes.	R

298
299
300
301

Table: XDR Document Metadata Attributes

S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2/O
1	Existing	author	Represents the provider NPI or institution NPI who authored the individual Document included in the Submission Set This attribute contains either the following sub-attributes and never both: authorInstitution authorPerson	R2
1.1	Existing	authorInstitution (sub-attribute of author)	Represents the NPI of the institution or the organization under which the human or machine authored the individual document included in the Submission Set. Please note: At the Document Metadata level, either the authorInstitution or authorPerson attribute shall be used but never both	R2
1.2	Existing	authorPerson (sub-attribute of author)	Represents the NPI of the provider who authored the individual document included in the submissionSet Please note: At the Document Metadata level, either the authorInstitution or authorPerson attribute shall be used but never both.	R2
2	Existing	classCode	The code that specifies the particular kind of document.	R
3	Existing	classCode DisplayName	The name to be displayed for communicating to a human the meaning of the classCode. Shall have a single value corresponding to the classCode used	R
4	Existing	comments	Comments associated with the Document in a free form text format	O
5	Existing	confidentialityCode	The code specifying the level of confidentiality of the Document.	R
6	Existing	creationTime	Represents the time the HIH created the document	R



S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2/O
7	Existing	entryUUID	A unique ID or a globally unique identifier for each document in the Submission Set	R
8	Existing	formatCode	Globally unique code for specifying the format of the document. For example, the format code for esMD is HITSP C62 urn:hitasp:c62:cda:pdf	R
9	Existing	Hash	Hash key of the C62 Document based on the SHA1 Hash Algorithm	R
10	Existing	healthcareFacility TypeCode	Represents the type of organizational or provider setting under which the documented act in the claim occurred	R
11	Existing	healthcareFacility TypeCodeDisplay Name	The name to be displayed for communicating to a human the meaning of the healthcareFacilityTypeCode. Shall have a single value corresponding to the healthcareFacilityTypeCode.	R
12	Existing	languageCode	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.	R
13	Existing	mimeType	MIME type of the document	R
14	Existing	patientId	<p>This is a required XDR field. Since esMD is Claim centric (and not Patient centric), esMD shall populate this field with Claim ID using the format Root + Extension. esMD shall include CMS OID as the root and Claim ID as the extension, like so:</p> <p>CMS OID.esMDClaimID</p> <p>Please, note: this value shall be the same as the one used at the Submission Set level.</p>	R
15	Existing	practiceSettingCode	<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 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>	R
16	Existing	practiceSettingCode DisplayName	<p>The name to be displayed for communicating to a human the meaning of the practiceSettingCode. Shall have a single value corresponding to the practiceSettingCode.</p> <p>This value will not be used by 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>	R
17	Existing	serviceStartTime	<p>Represents the start time of the provider service being documented.</p> <p>This value will not be used by esMD (i.e., will be</p>	R



S.No	Existing or Extension	esMD XDR Metadata Attribute	Definition	R/R2/O
			ignored). However, since this field is required by XDR, an input is required. Any possible value assigned by the sender will be accepted.	
18	Existing	serviceStopTime	Represents the stop time of the provider service being documented. This value will not be used by 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.	R
19	Existing	size	Size in bytes of the C62 attachment byte stream that was provided through the request.	R
20	Existing	title	Represents the title of the document. Max length shall be 128 bytes in UTF-8 format.	O
21	Existing	typeCode	The code specifying the precise kind of document (e.g., Claim Document Summary, ADR, ADMC, Progress Notes, Orders, Appeal Request).	R
22	Existing	typeCodeDisplay Name	The name to be displayed for communicating to a human the meaning of the typeCode. Shall have a single value corresponding to the typeCode.	R
23	Existing	uniqueId	A globally unique identifier assigned by the HIH to each document in the submission set. The length of the Unique Identifier shall not exceed 128 bytes. The structure and format of this ID shall be consistent with the specification corresponding to the format attribute. This ID will be generated based on the UUID.	R

302

3.3 Extra Metadata Elements

303

304

305

306

307

308

309

The submitter shall include two additional metadata slots for transactions submitted to esMD. The slot syntax and requirements shall conform to the specifications for extra metadata elements contained in the IHE ITI TF-3 Rev. 6.0 for XDS transmissions. These additional attributes will be prefixed with urn:nhin:esMD to distinguish them from the existing IHE XDR attributes.

310

The table below specifies these esMD specific attributes.

311

312

313

314

315

316

317

318

319

320

321



322 **Table 1 – esMD specific extra Metadata Elements** (This metadata was added to above Submission Set Metadata
323 table)
324

S.No	esMD XDR Metadata Attribute (Slot)	Definition	R/R2/O
1	urn:nhin:esMD:ClaimId	Metadata Slot to contain the number of the claim associated with the response package being submitted. This could be found in the Additional Documentation Request (ADR) letter sent by the Review Contractor if the request is from Medicare Audit Contractor (MAC). This additional slot shall be part of the SubmissionSet.	R
2	urn:nhin:esMD:CaseId	Metadata Slot to contain the identification number assigned by the Medicare contractor who made the additional documentation request. This could be found in the Additional Documentation Request (ADR) letter from the Review Contractor if the request is from Medicare Audit Contractor (MAC). This additional slot shall be part of the SubmissionSet.	R2

325

326 4 Acknowledgment and Responses (Status and Notification Messages)

327

328 esMD implements the NHIN Document Submission with Deferred Messaging mode.

329

330 In a deferred mode, the Document Submission is a two-way message as shown in the diagram below:

331

332 1) Using the Health Information Handler (HIH) Gateway, provider submits a claim document
333 response to a single CMS Additional Documentation Request Letter (ADR), using the Document
334 Submission deferred request (as a part of deferred messaging flow). For this, HIH Gateway
335 establishes a new secure HTTP connection to CMS esMD Gateway. The SOAP action for this
336 deferred document submission request is
337 **urn:nhin:Deferred:ProvideAndRegisterDocumentSet-b.**

338

339 2) The CMS esMD Gateway uses the same secure HTTP connection (in message number 1) to
340 send the response to the HIH gateway, and which is a Document Submission deferred Request
341 Acknowledgement message. It leverages the ebxml Registry Response element with a status
342 code of *urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:RequestAccepted*. Any errors
343 that occur prior to the processing of the esMD metadata, Payload and ECM Delivery provided in
344 message number 1 will be communicated via a soap fault. The SOAP action for the deferred
345 document submission request acknowledgement is
346 **urn:nhin:Deferred:ProvideAndRegisterDocumentSet-bAcknowledgement**

347

348 This Acknowledgment message will be sent to the HIH gateway after successful two-way TLS
349 authentication between HIH and esMD Gateways, and esMD Gateway SAML Assertion
350 validation.

351

352 3) The CMS esMD Gateway establishes a new secure HTTP connection to the HIH Gateway and
353 submits the esMD Document Submission deferred Response with Processing and ECM Delivery
354 status notification message content. The SOAP action for this message is
355 **urn:nhin:Deferred:ProvideAndRegisterDocumentSet-bResponse.**

356
357 Based on following validations and processes, this document submission deferred response
358 message will be sent to HIH from CMS Gateway along with the original document submission
359 deferred request message ID, unique ID, its esMD generated transaction ID (in the case of
360 successful OID validation), Request Type (OID Authorization, ECM Delivery and Review
361 Contractor Pickup), and status details.

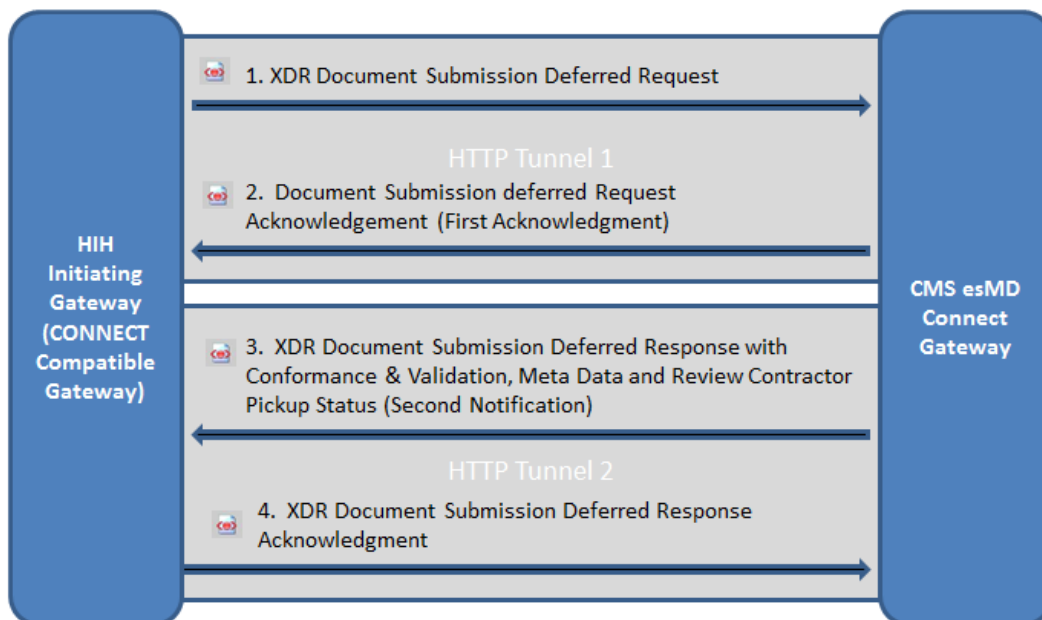
362 **Validation:**

- 363 • Validate the Unique ID of the message to avoid duplicate submission
- 364 • Validate the OID authorization based on CMS On-boarding
- 365 • Validate the participation of the intended recipient (i.e., the Review Contractor)
- 366 • Validate the syntaxes
- 367 • Validate the Semantics against esMD affinity domain specific values

368 **Process:**

- 369 • Persist Metadata into CMS esMD metadata database
- 370 • Deliver provider submitted claim document/s to CMS Enterprise Content Management
- 371 (ECM) repository
- 372 • Review Contractor picks up the submitted documents from the CMS ECM repository

- 373
374
375
376 4) The HIH Gateway uses the same secure HTTP connection (in message number 3) and sends a
377 response as a Document Submission Response Acknowledgment message. It leverages the
378 ebxml RegistryResponse element with a status of *urn:oasis:names:tc:ebxml-*
379 *regrep:ResponseStatusType:ResponseAccepted*. Any errors that occur during the processing of
380 the registry response message (message 3) shall be communicated via a soap fault. The SOAP
381 action for the deferred Document Submission response acknowledgement is
382 **urn:nhin:Deferred:ProvideAndRegisterDocumentSet-bResponseAcknowledgement**.



386
387
388



389 **Figure: XDR Document Submission Message Flow – In Deferred Message Mode**
390
391 Note: In the future, esMD would like to enhance the response notification using a more meaningful and
392 realistic workflow status notifications flow.
393
394 esMD XDR Profile implementation at CMS Gateway, makes no assumption on the amount of time that
395 may transpire and, in fact, should allow for long latency on the response. In some cases, that could be
396 hours or days. The main point here is that the esMD XDR submitter (Client) is able to move on to other
397 things while the submission is being processed at the CMS Gateway server.

398
399 **5 Error Handling**
400
401 Error codes are defined in section 4 of *Integrating the Healthcare Enterprise's (IHE's) Information*
402 *Technology Industry (ITI) Technical Framework*, Volume 3. The esMD profile will reuse the following XDR
403 error codes. The following table shows the error, the error code, and a description of information which
404 will populate in the RegistryError text field.

405 **Table 2 - Error Codes**

406

Error	Existing or Extension	Error Code	Description
Document not well formed or Internal esMD or Infrastructure issues	Existing	XDSRepositoryError	The document does not conform to esMD Profile.
Double Submission	Existing	XDSDuplicateUniqueldInRegistry	Uniqueld received was not unique. Uniqueld could have been attached to earlier XDSSubmissionSet .
XDR Submission Set Metadata Error	Existing	XDSRegistryMetadataError	List violating elements if possible.
XDS Document Metadata is missing	Existing	XDSMissingDocumentMetadata	Error detected in XDR document metadata.
Missing Attachment	Existing	XDSMissingDocument	XDSDocumentEntry exists in metadata with no corresponding attached document.
Encryption Failed - Integrity of the submitted attachment	Existing	XDSNonIdenticalHash	The attached document and hash code does not match. Or could have been tampered with over the transmission.

407

408
409 **6 esMD C62 Context Overview**
410 The document body of a C62 CDA will include an unstructured (e.g., UTF8 Text) presentation preserved
411 format, such as PDF file. The PDF document format is further specified in the International Organization
412 for Standardization (ISO) PDF/A ISO#19005-1b, Document management - Electronic document file
413 format for long-term preservation standard.
414 Examples of documents that would be embedded in the HITSP C62 include PDF formats.



Electronic Submission of Medical Documentation (esMD)
Production Specification v1.0



415 Note: esMD XDR Profile will not support TIFF documents until HITSP C62 profile is updated to reflect
416 TIFF support. Possibly in the future, esMD XDR Profile might support TIFF format.
417
418
419
420



421
422
423
424

Table 3 - esMD C62 Standards

esMD C62 Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Cross Enterprise Sharing of Scanned Documents (XDS-SD) Integration Profile	This Integration Profile defines how to store healthcare metadata in clinical documents, including patient identifiers, demographics, encounter, order or service information, represented within a structured HL7 CDA R2 header, with a PDF or plaintext formatted document containing clinical information within a nonXMLBody. For more information visit www.ihe.net to retrieve Volume 1, and Volume 2 of the Framework
International Organization for Standardization (ISO) PDF/A ISO 19005-1b. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF (PDF/A)	Specifies how to use the Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster and vector data. For more information visit www.iso.org

425 **6.1 Submission Specifications**

426 This profile describes how to use C62 format to foster submission of medical documentation requested by
427 the Medicare Review Contractor. This profile:

- 428 • References underlying C62 Section Content Modules and Entry Content Modules
- 429 • Specifies constraints and other rules for using the formats, and
- 430 • Specifies additional constraints for using standard vocabularies and code sets where
431 applicable.

432 The profile does not intend to detail XDR and HITSP C62 implementation constraints but rather directs
433 implementers to HITSP C62 messaging Content Modules Component for conformance specifications.

434
435
436

Table 4- Summary of esMD Specification

Content Module	C62
Personal Information	R
Reason for Referral	X
History of Present Illness	X
Active Problems	X
Hospital Course	X
Plan of Care	X
Attachments in PDF	R
Order Msg for drugs, labs, DME	X
Physical Exam	X
Vital Signs	X
Review of Systems	X
Diagnostic Results	X
Test Results	X
Functional Status	X
Progress Note	X
Medications Administered	X
Chief Complaint	X



Content Module	C62
Reason for Visit	X
Allergies and Other Adverse	X
Medications (incl. Current Meds)	X
Admissions Medication History	X
Hospital Discharge Medications	X
IV Fluids Administered	X
Problem List	X
Conditions	X
History of Past Illness	X
Hospital Admission Diagnosis	X
ED Diagnoses	X
List of Surgeries/Procedures	X
Procedures Performed	X
Discharge Diet	X
Advance Directives	X
Immunizations	X
Assessments	X
Assessment and Plan	X
Family History	X
Social History	X
Encounters	X
Medical Equipment	X
Referral Source	X
Mode of Arrival	X
Consultations	X
ED Disposition	X
Payers	X
Information Source	X
Language Spoken	X
Support	X
Healthcare Provider	X
Pregnancy	X
Comment	X
Purpose	X

437
438

439 **6.2 Attachments in the esMD C62 Format**

- 440 The following constraints apply to the C62 attachments. The file must be in .pdf format.
- 441 a. The message size must not exceed 19 mb.
 - 442 b. At least one file must be attached to a C62.
 - 443 c. Multiple files may be attached to a single XDR SOAP Message.

444
445
446
447
448
449
450



451 **7 GLOSSARY**

452
453 **Electronic Submission of Medical Documentation**

454
455 **Health Information Handler (HIH)**

456
457 A Health Information Handler (HIH) is defined as an organization that oversees and governs the
458 exchange of health-related claim reviewer information from Provider to CMS esMD Gateway according to
459 nationally recognized standards.¹

460
461 **Interoperability**

462
463 Interoperability is the ability of health information systems to work together, within and across
464 organizational boundaries, in order to advance the effective delivery of healthcare for individuals and
465 communities.

466
467 **Nationwide Health Information Network (NHIN)**

468 The Nationwide Health Information Network (NHIN) is a set of standards, protocols, legal agreements,
469 and specifications that a consortium of health information organizations have agreed are necessary for
470 secure and private exchange of health information over the internet. The NHIN is overseen by the Office
471 of the National Coordinator for Health IT (ONC).

472 **NHIN Exchange**

473 The NHIN Exchange is designed to connect a diverse set of federal agencies and private organizations to
474 securely exchange electronic health information. CMS believes the NHIN Exchange holds promise and
475 intends to use it during the esMD pilot. More information on NHIN Exchange can be found by clicking the
476 "NHIN Exchange" link below.

477 **Nonfunctional Requirement (NR)**

478
479 An NR is a low-level requirement that focuses on the specific characteristics that must be addressed in
480 order to be acceptable as an end product. NRs have a focus on messaging, security, and system
481 interaction.

482
483 **Privacy**

484
485 An individual's interest in protecting his or her individually identifiable health information and the
486 corresponding obligation of those persons and entities, that participate in a network for the purposes of
487 electronic exchange of such information, to respect those interests through fair information practices.

488
489 **Security**

490
491 The physical, technological, and administrative safeguards used to protect individually identifiable health
492 information.

493
494
495 **Acknowledgement (ACK)**

¹ The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms April 28, 2008



496
497 Message (such as one used in 'handshaking' process between two systems) that indicates the status of
498 communications received. Commonly written as *ACK*.

499
500 **HTTPs**

501
502 A set of rules for speedy retrieval and transmission of electronic documents written in HTML over a
503 secure connection. HTTPS addresses differentiate from HTTP ones because they encrypt and decrypt
504 user pages to prevent unauthorized access to sensitive data. Online credit card processing and banking
505 websites use HTTPS addresses to ensure privacy and provide secure processing for users.

506
507 **TLS**

508
509 Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic
510 protocols that "provide communications security over the Internet". TLS and SSL encrypt the segments of
511 network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed
512 message authentication code for message reliability. TLS is an IETF standards track protocol, last
513 updated in RFC 5246, and is based on the earlier SSL specifications developed by Netscape
514 Corporation.

515
516 The TLS protocol allows client/server applications to communicate across a network in a way designed to
517 prevent eavesdropping and tampering. A TLS client and server negotiate a stateful connection by using a
518 handshaking procedure. During this handshake, the client and server agree on various parameters used
519 to establish the connection's security.

- 520
- 521 • The handshake begins when a client connects to a TLS-enabled server requesting a secure
522 connection, and presents a list of supported CipherSuites (ciphers and hash functions).
 - 523 • From this list, the server picks the strongest cipher and hash function that it also supports and
524 notifies the client of the decision.
 - 525 • The server sends back its identification in the form of a digital certificate. The certificate usually
526 contains the server name, the trusted certificate authority (CA), and the server's public encryption
527 key.
 - 528 • The client may contact the server that issued the certificate (the trusted CA as above) and
529 confirm that the certificate is valid before proceeding.
 - 530 • In order to generate the session keys used for the secure connection, the client encrypts a
531 random number (RN) with the server's public key (PbK), and sends the result to the server. Only
532 the server should be able to decrypt it (with its private key (PvK)): this is the one fact that makes
533 the keys hidden from third parties, since only the server and the client have access to this data.
534 The client knows PbK and RN, and the server knows PvK and (after decryption of the client's
535 message) RN. A third party is only able to know RN if PvK has been compromised.
 - 536 • From the random number, both parties generate key material for encryption and decryption.
 - 537 • This concludes the handshake and begins the secured connection, which is encrypted and
538 decrypted with the key material until the connection closes.

539
540 If any one of the above steps fails, the TLS handshake fails, and the connection is not created.

541
542 **SAML**

543
544 Security Assertion Markup Language used for message authentication.

545
546
547
548 **Interface**



549 A well-defined boundary where direct contact between two different environments, systems, etc., occurs,
550 and where information is exchanged.

551 **SOAP**

552 Simple Object Access Protocol is a message exchange format for web services.

553 **Transaction**

554 Event or process (such as an input message) initiated or invoked by a user or system, regarded as a
555 single unit of work and requiring a record to be generated for processing in a database.

556 **Performance**

557 Accomplishment of a transaction measured against preset standards of accuracy, completeness, cost,
558 and speed.

559 **Response Time**

560 It is the interval between a user-command and the receipt of an action, result, or feedback from the
561 system. It is expressed as the sum of (a) transmission time of the command to the system, (b) processing
562 time at the CPU, (c) access time to obtain required data from a storage device, and (d) transmission time
563 of the result back to the user. When applied to a system component, it is the time taken to react to a
564 system request or a given input.

565 **8 ACRONYMS**

566 CMS	Centers for Medicare & Medicaid Services
567 HIPAA	Health Information Portability and Accountability Act
568 HIT	Health Information Technology
569 HITSP	Health Information Technology Standards Panel
570 HL7	Health Level 7
571 HIH	Health Information Handler
572 HTTP	Hypertext Transfer Protocol
573 HTTPS	Hypertext Transfer Protocol Secured
574 ICD	Interface Control Document
575 NHIN	Nationwide Health Information Network
NR	Nonfunctional Requirement
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
OASIS	Outcome Assessment Information Set
XML	Extensible Markup Language



Electronic Submission of Medical Documentation (esMD)
Production Specification v1.0



576 The 508 compliance standards address access to all information, documentation, and support provided to end users
577 (e.g., Federal employees) of covered technologies. The information contained in this document is in compliance with
578 508 standards, and is available in alternate formats, upon request, at no additional charge.

579