CAQH Committee on Operating Rules for Information Exchange (CORE)
Draft CAQH CORE Attachments (275/278) Infrastructure Rule
Draft for CAQH CORE ASG-PA Straw Poll #2

Table of Contents

1   **3   Scope**

2   *3.1. What the Rule Applies To*

3   This CAQH CORE Attachments (275/278) Prior Authorization Infrastructure Rule applies to the conduct
4   of the following X12 transactions:

5   • X12 005010X217 278 Health Care Services Review – Request for Review and Response Technical
6   Report Type 3 and associated errata (hereafter referenced as X12 v5010X217 278).
7   • X12 006020X316 275 Additional Information to Support a Health Care Services Review Technical
8   Report Type 3 (hereafter referenced as X12 v6020X316 275).
9   • X12 006020X290 999 Implementation Acknowledgement for Health Care Insurance Technical
10   Report Type 3 (hereafter referenced as X12 v6020X290 999).
11   • X12 006020X257 824 Application Advice Technical Report Type 3 (hereafter referenced as X12
12   v6020X257 824).
13
14   This rule optionally applies to other payload types (e.g., HL7 C-CDA, .pdf, etc.) and to non-X12 payload
15   exchange scenarios (e.g., CORE Connectivity, FHIR, etc.).

16   *3.2. When the Rule Applies*

17   This CAQH CORE Attachments (275/278) Prior Authorization Infrastructure Rule applies when:

18   • A provider and its agent electronically send patient-specific medical information or
19   supplemental documentation (solicited or unsolicited) to a health plan and its agent to support
20   a X12 v5010X217 278 Prior Authorization Request.

21   And

22   • A health plan and its agent electronically process patient-specific medical information or
23   supplemental documentation and respond to a provider and its agent to support a X12
24   v5010X217 278 Prior Authorization Response.

25   *3.3. What the Rule Does Not Require*

26   While the rule requirements address the optional use of non-X12 additional documentation submission
27   methods, the rule does not require any entity and its agent to:

28   • Exchange documentation using an electronic, non-X12 additional documentation submission
29   method (e.g., HL7 C-CDA, .pdf, .doc, etc.) exchanged via CORE Connectivity Rule vC4.0.0.

30   *3.4. Outside the Scope of This Rule*

31   This rule does not address any data content requirements of the X12 v6020X316 275 transaction. This
32   CAQH CORE Attachments (275/278) Prior Authorization Infrastructure Rule is applicable to improving
33   access for additional information to support a Health Care Services Review and Request and not
34   addressing data content requirements for transactions identified in Section 3.1.

3.5. Maintenance of This Rule

Any substantive updates to this rule (i.e., change to rule requirements) will be made in alignment with federal processes for updating versions of the operating rules, as determined by industry need, or by CAQH CORE Participants.

3.6. Assumptions

A goal of this rule is to adhere to the principles of electronic data interchange (EDI) in assuring that transactions sent are accurately received and to facilitate correction of errors for electronically submitted additional documentation requests.

The following assumptions apply to this rule:

- A successful communication connection has been established.
- This rule is a component of the larger set of CAQH CORE Operating Rules; as such, all the CAQH CORE Guiding Principles apply to this rule and all other rules.
- This rule is not a comprehensive companion document addressing any content requirements of the X12 v6020X316 275 Additional Information to Support a Health Care Services Review transactions, X12 v5010X217 278, X12 v6020X290 999 or X12 v6020X257 824.
- Compliance with all CAQH CORE Operating Rules is a minimum requirement; any HIPAA-covered entity is free to offer more than what is required in the rule.

4 Infrastructure Rule Requirements for Attachments using the X12 275 Transaction

4.1. Processing Mode Requirements for X12 275 Attachments

A HIPAA-covered health plan and its agent must implement the server requirements for Batch Processing Mode for the X12 v6020X316 275 Attachment transaction as specified in the CAQH CORE Connectivity Rule vC4.0.0. Additionally, a HIPAA-covered health plan and its agent must implement the server requirements for Real Time Processing Modes as specified in the CAQH CORE Connectivity Rule vC4.0.0.

A HIPAA-covered health plan and its agent conducting the X12 v6020X316 275 Attachment transaction is required to conform to the processing mode requirements specified in this section regardless of any other connectivity modes and methods used between trading partners.

4.2. Connectivity Requirements for X12 275 Attachments[1]

A HIPAA-covered entity and its agent must be able to support the CAQH CORE Connectivity Rule vC4.0.0.

This connectivity rule addresses usage patterns for Real Time and Batch Processing Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message payload exchanges beyond declaring the formats that must be used between entities and that security information must be sent outside of the message envelope payload.

---

[1] The HL7 CDA R2 Attachment Implementation Guide: Exchange of C-CDA Based Documents, Release 1 describes standards based approaches to sending a CDA Document for Attachments using electronic transactions in Appendix F, including CORE Connectivity + X12 275.

69 All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in the
70 CAQH CORE Connectivity Rule vC4.0.0. The CAQH CORE Connectivity Rule vC4.0.0 is designed to provide
71 a "Safe Harbor" that application vendors, HIPAA-covered providers and their agents and HIPAA-covered
72 health plans and their agents (or other information sources) can be assured will be supported by any
73 trading partner. Supported means that the entity is capable and ready at the time of the request by a
74 trading partner to exchange data using the CAQH CORE Connectivity Rule vC4.0.0. These requirements
75 are not intended to require trading partners to remove existing connections that do not match the rule,
76 nor are they intended to require that all trading partners must use this method for all new connections.
77 CAQH CORE expects that in some technical circumstances, trading partners may agree to use different
78 communication mechanism(s) and/or security requirements than those described by these
79 requirements.

80 The requirement to support the CAQH CORE Connectivity Rule vC4.0.0 does not apply to retail
81 pharmacy. For retail pharmacy the entity should reference the NCPDP Connectivity Operating Rule v1.0
82 that can be obtained from www.ncpdp.org. NCPDP and CAQH CORE support a shared goal of continued
83 alignment for connectivity across retail pharmacy and medical.

84 ### 4.3. System Availability and Reporting Requirements for X12 275 Attachments

85 Many healthcare providers have a need to send additional information to support prior
86 authorizations outside of the typical business day and business hours. Additionally, many
87 institutional providers are now allocating staff resources to performing administrative and
88 financial back-office activities on weekends and evenings. As a result, providers have a
89 business need to be able to submit additional information to support a prior authorization
90 transaction at any time.

91 On the other hand, HIPAA-covered health plans have a business need to periodically take
92 their additional information processing and other systems offline to perform required system
93 maintenance. This typically results in some systems not being available for timely processing
94 of X12 v6020X316 275 Additional Information and X12 v6020X290 999 on certain nights and
95 weekends. This rule requirement addresses these conflicting needs.

96 #### 4.3.1. System Availability Requirements

97 System availability must be no less than 86 percent per calendar week for both Real Time
98 and Batch Processing Modes. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m.
99 the following Sunday. This will allow for a HIPAA-covered health plan and its agent to
100 schedule system updates to take place within a maximum of 24 hours per calendar week
101 for regularly scheduled downtime.

102 #### 4.3.2. Reporting Requirements

103 ##### 4.3.2.1. Scheduled Downtime

104 A HIPAA-covered health plan and its agent must publish its regularly scheduled system
105 downtime in an appropriate manner (e.g., on websites or in Companion Guides) such that
106 the HIPAA-covered health plan's trading partners can determine the health plan's system
107 availability so that staffing levels can be effectively managed.

108   ***4.3.2.2.   Non-Routine Downtime***

109   For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan and its
110   agent must publish the schedule of non-routine downtime at least one week in advance.

111   ***4.3.2.3.   Unscheduled Downtime***

112   For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan
113   and its agent are required to provide information within one hour of realizing downtime will
114   be needed.

115   ***4.3.2.4.   No Response Required***

116   No response is required during scheduled, non-routine, or unscheduled downtime(s).

117   ***4.3.2.5.   Holiday Schedule***

118   Each HIPAA-covered health plan and its agent will establish its own holiday schedule
119   and publish it in accordance with the rule requirements above.

120   ***4.4. Payload Acknowledgements and Response Time Requirements for X12 275 Attachments***

121   Providers are often not aware whether an attachment sent to support a prior authorization Request was
122   received. As a result, providers often re-send the attachment or revert to manual processes (e.g., fax,
123   phone, etc.) to determine the status of the prior authorization Request and corresponding attachment.
124   The following rule requirements address the method and response time for a health plan and its agent
125   to return an acknowledgement of receipt to providers and their agents when sending a X12 v6020X316
126   275 or non-X12 attachment (e.g., HL7 C-CDA, PDF, etc.).

127   ***4.4.1. Payload Acknowledgements for X12 275 Attachments***

128   ***4.4.1.1.   Use of the X12 999 Implementation Acknowledgement***

129   The requirements in this section apply to a HIPAA-covered health plan and its agent when it receives an
130   X12 v6020X316 275 in real time or batch.

131   When any Functional Group of a X12 v6020X316 275 Attachment Transaction Set is accepted,
132   accepted with errors, or rejected the HIPAA-covered health plan and its agent must return a
133   X12 v6020X290 999 transaction. The X12 v6020X290 999 transaction must report each error
134   detected to the most specific level of detail supported by the X12 v6020X290 999 transaction.

135   ***4.4.1.2.   Response Time Requirements for Availability of Acknowledgements***

136   Each HIPAA-covered entity and its agent must support this maximum response time requirement to
137   ensure that at least 90 percent of all required responses are returned within the specified maximum
138   response time as measured within a calendar month.

139   Each HIPAA-covered entity and its agent must capture, log, audit, match, and report the date
140   (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the
141   corresponding data received from its trading partners.

142   Each HIPAA-covered entity and its agent must support these response time requirements in this section
143   and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between
144   trading partners.

145   ### *4.4.1.3.   Batch Mode Response Time Requirements*

146 Maximum elapsed time for the availability of an X12 v6020X290 999 transaction to any X12 v6020X316
147 275 Attachment transaction that is submitted by a provider, or on a provider's behalf by a
148 clearinghouse/switch in Batch Processing Mode, by 9:00 pm Eastern Time of a business day must be no
149 later than 7:00 am Eastern Time the second business day following submission.
150
151 A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each
152 designated day through 11:59 pm (2359 hours) of that same designated day. The actual calendar day(s)
153 constituting business days are defined by and at the discretion of each HIPAA-covered health plan and
154 its agent.

155   ### *4.4.1.4.   Real Time Response Time Requirement*

156 *Maximum* response time for the receipt of an X12 v6020X290 999 Response from the time of
157 submission of an X12 v6020X316 275 must be 20 seconds when processing in Real Time Processing
158 Mode. The recommended maximum response time between each participant in the transaction routing
159 path is 4 seconds or less per hop as long as the 20-second total roundtrip *maximum* requirement is met.

160   ### *4.4.1.5.   Basic Requirements for Receivers of Acknowledgments*

161 The receiver (defined in the context of this CAQH CORE Operating Rule as the HIPAA-covered provider
162 and its agent) of an X12 v6020X290 999 transaction is required:

163 • To process any X12 v6020X290 999 transaction within one business day of its receipt

164   And

165 • To recognize all error conditions that can be specified using all standard acknowledgements
166   named in this rule

167   And

168 • To pass all such error conditions to the end user as appropriate

169   Or

170 • To display to the end user text that uniquely describes the specific error condition(s),
171   ensuring that the actual wording of the text displayed accurately represents the error
172   code and the corresponding error description specified in the related X12 v6020X290
173   999 specification without changing the meaning and intent of the error condition
174   description.

175 The actual wording of the text displayed is at the discretion of the HIPAA-covered provider and its
176 agent.

177   ### *4.5. File Size Requirements for X12 275 Attachments*

178 Each HIPAA-covered entity and its agent must support the receipt and processing of the *minimum*
179 sizing requirements to ensure attachments can be processed across varying systems.

180   ### *4.5.1. Front End Server File Size Requirements for Attachments using an X12 275 Transaction*

181 A HIPAA-covered entity and its agent must be able to accept a *Minimum* 64MB of Base64 encoded data
182 by their front-end servers when the encoded data received is exchanged via the X12 v6020X316 275
183 transaction.

184 ### *4.5.2. Internal Document Management Systems File Size Requirement Pertaining to*
185 ### *Attachments using an X12 275 Transaction*

186 A HIPAA-covered entity and its agent must be able to accept a *Minimum* 64MB file size document by
187 their internal document management systems.

188 ## *4.6. Companion Guide for X12 275 Attachments*

189 A HIPAA-covered health plan and its agent have the option of creating a "Companion Guide" that
190 describes the specifics of how it will implement the X12 transactions. The Companion Guide is in
191 addition to and supplements the X12 TR3 Implementation Guide.

192 Currently HIPAA-covered health plans and their agents have independently created Companion Guides
193 that vary in format and structure. Such variance can be confusing to trading partners/providers who
194 must review numerous Companion Guides along with the X12 TR3 Implementation Guides. To address
195 this issue, CAQH CORE developed the CAQH CORE Master Companion Guide Template for health plans
196 and information sources. Using this template, health plans and information sources can ensure that the
197 structure of their Companion Guide is similar to other health plan's documents, making it easier for
198 providers to find information quickly as they consult each health plan's document on these important
199 industry EDI transactions.

200 Developed with input from multiple health plans, system vendors, provider representatives, and health
201 care industry experts, this template organizes information into several simple sections – General
202 Information (Sections 1-9) and Transaction-Specific Information (Section 10) – accompanied by an
203 appendix. Note that the Companion Guide template is presented in the form of an example from the
204 viewpoint of a fictitious Acme Health Plan.

205 Although CAQH CORE believes that a standard template/common structure is desirable, it recognizes
206 that different HIPAA-covered health plans may have different requirements. The CAQH CORE Master
207 Companion Guide template gives health plans the flexibility to tailor the document to meet their
208 particular needs.

209 The requirements specified in this section do not currently apply to retail pharmacy.

210 ### *4.6.1. Companion Guide Requirements for X12 275 Attachments*

211 If a HIPAA-covered entity and its agent publishes a Companion Guide covering the X12 v6020X316 275,
212 the Companion Guide must follow the format/flow as defined in the CAQH CORE Master Companion
213 Guide Template for X12 Transactions (CAQH CORE Master Companion Guide Template available HERE).

214 **NOTE**: This rule does not require any HIPAA-covered entity to modify any existing Companion Guides
215 that cover HIPAA-mandated/non-HIPAA-mandated transactions.

216 **5** **Infrastructure Rule Requirements for Additional Documentation using the Non-X12 Method**

217 *5.1. Connectivity Requirements for Additional Documentation using CORE Connectivity*

218 If a HIPAA-covered entity and its agent elect to use CORE Connectivity as their non-X12 method of
219 additional documentation submission, the CAQH CORE Connectivity Rule vC4.0.0[2] must be supported.

220 This connectivity rule addresses SOAP and REST usage patterns for Real Time and Batch Processing
221 Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It
222 does not attempt to define the specific content of the message payload exchanges beyond declaring the
223 formats that must be used between entities and that security information must be sent outside of the
224 message envelope payload.

225 All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in the
226 CAQH CORE Connectivity Rule vC4.0.0. The CAQH CORE Connectivity Rule vC4.0.0 is designed to provide
227 a "Safe Harbor" that application vendors, HIPAA-covered providers and their agents and HIPAA-covered
228 health plans and their agents (or other information sources) can be assured will be supported by any
229 trading partner. Supported means that the entity is capable and ready at the time of the request by a
230 trading partner to exchange data using the CAQH CORE Connectivity Rule vC4.0.0. These requirements
231 are not intended to require trading partners to remove existing connections that do not match the rule,
232 nor are they intended to require that all trading partners must use this method for all new connections.
233 CAQH CORE expects that in some technical circumstances, trading partners may agree to use different
234 communication mechanism(s) and/or security requirements than those described by these
235 requirements.

236 The requirement to support the CAQH CORE Connectivity Rule vC4.0.0 does not apply to retail
237 pharmacy. For retail pharmacy the entity should reference the NCPDP Connectivity Operating Rule v1.0
238 that can be obtained from www.ncpdp.org. NCPDP and CAQH CORE support a shared goal of continued
239 alignment for connectivity across retail pharmacy and medical.

240 *5.2. System Availability and Reporting Requirements for Additional Documentation using the*
241 *Non-X12 Method*

242 Many healthcare providers have a need to send additional information to support prior
243 authorizations outside of the typical business day and business hours. Additionally, many
244 institutional providers are now allocating staff resources to performing administrative and
245 financial back-office activities on weekends and evenings. As a result, providers have a
246 business need to be able to submit additional information to support a prior authorization
247 transaction at any time.

248 On the other hand, HIPAA-covered health plans have a business need to periodically take
249 their additional information processing and other systems offline to perform required system
250 maintenance. This typically results in some systems not being available for timely processing
251 of additional information or documentation on certain nights and weekends. This rule
252 requirement addresses these conflicting needs.

---

[2] CORE Connectivity vC4.0.0 specifies requirements for the exchange of messages using SOAP and REST.
Additionally, CORE Connectivity is payload agnostic, meaning the SOAP and REST Services are not aware of the
content they are serving.

253   ### *5.2.1. System Availability Requirements*

254   System availability must be no less than 86 percent per calendar week for both Real Time
255   and Batch Processing Modes. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m.
256   the following Sunday. This will allow for a HIPAA-covered health plan and its agent to
257   schedule system updates to take place within a maximum of 24 hours per calendar week
258   for regularly scheduled downtime.

259   ### *5.2.2. Reporting Requirements*

260   #### *5.2.2.1. Scheduled Downtime*

261   A HIPAA-covered health plan and its agent must publish its regularly scheduled system
262   downtime in an appropriate manner (e.g., on websites) such that the HIPAA-covered health
263   plan's trading partners can determine the health plan's system availability so that staffing
264   levels can be effectively managed.

265   #### *5.2.2.2. Non-Routine Downtime*

266   For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan and its
267   agent must publish the schedule of non-routine downtime at least one week in advance.

268   #### *5.2.2.3. Unscheduled Downtime*

269   For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan
270   and its agent are required to provide information within one hour of realizing downtime will
271   be needed.

272   #### *5.2.2.4. No Response Required*

273   No response is required during scheduled, non-routine, or unscheduled downtime(s).

274   #### *5.2.2.5. Holiday Schedule*

275   Each HIPAA-covered health plan and its agent will establish its own holiday schedule
276   and publish it in accordance with the rule requirements above.

277   ### *5.3. Payload Acknowledgements Requirements for Additional Documentation using the Non-X12*
278   *Method*

279   Providers are often not aware whether an attachment sent to support a prior authorization Request was
280   received. As a result, providers often re-send the attachment or revert to manual processes (e.g., fax,
281   phone, etc.) to determine the status of the prior authorization Request and corresponding attachment.
282   The following rule requirements address the method and response time for health plans to return an
283   acknowledgement of receipt to providers when sending a non-X12 attachment (e.g., HL7 C-CDA, PDF,
284   etc.).

285   ### *5.3.1. Payload Acknowledgement Requirements – Use of the X12 278 Response*

286   Additional documentation sent via a non-X12 method cannot be acknowledged by X12 v6020X290 999.
287   Therefore, health plan and their agents will send a X12 v5010X217 278 Response following the [CAQH
288   CORE Prior Authorization & Referrals (278) Infrastructure Rule vPA2.0](#) and [CAQH CORE Prior
289   Authorization & Referrals (278) Data Content Rule vPA1.0](#) to notify providers and their agent that the

290   original X12 v5010X217 278 Request, and any associated additional documentation sent to support the
291   278 Request, was approved, denied, or pended for additional information.

292

293   **5.4. File Size Requirements for Additional Documentation using the Non-X12 Method**

294   Each HIPAA-covered entity and its agent must support the receipt and processing of the *minimum*
295   sizing requirements to ensure attachments can be processed across varying systems.

296   **5.4.1. Front End Server File Size Requirements for Additional Documentation using the Non-**
297   **X12 Method**

298   A HIPAA-covered entity and its agent must be able to accept a *Minimum* 64MB of Base64 encoded data
299   by their front-end servers when the encoded data received is exchanged via a non-X12 method.

300   **5.4.2. Internal Document Management Systems File Size Requirement Pertaining to**
301   **Additional Documentation using the Non-X12 Methods**

302   A HIPAA-covered entity and its agent must be able to accept a *Minimum* 64MB file size document by
303   their internal document management systems.