



## CORE Phase I Eligibility and Benefits Operating Rules Manual

Approved April 2006

## CORE Phase I Eligibility and Benefits Policies and Rules

Contact CAQH for more information:

CAQH  
601 Pennsylvania Avenue, NW  
South Building, Suite 500  
Washington, DC 20004  
(202) 861-6380  
[CORE@caqh.org](mailto:CORE@caqh.org)

[www.caqh.org](http://www.caqh.org)

If you have any questions or identify any problems please call CAQH at (202) 861-6380

# CORE Phase I Eligibility and Benefits Policies and Rules

## Table of Contents

### CORE Phase I Policies (100-105)

<b>100</b>	<b>Guiding Principles</b> .....	<b>1</b>
<b>101</b>	<b>Pledge<sup>1</sup></b> .....	<b>4</b>
<b>102</b>	<b>Certification Policy</b> .....	<b>6</b>
	<i>Section 1: Fees<sup>2</sup></i> .....	<i>7</i>
	<i>Section 2: Period for Which Certification Applies</i> .....	<i>7</i>
	<i>Section 3: Key Steps</i> .....	<i>7</i>
	<i>Section 4: Certification Testing Appeals Process</i> .....	<i>9</i>
	<i>HIPAA Attestation Form<sup>1</sup></i> .....	<i>10</i>
<b>103</b>	<b>Exemption Policy</b> .....	<b>11</b>
	<i>Section 1: Required Criteria to be Granted a CORE Health Plan IT System Exemption</i> .....	<i>11</i>
	<i>Section 2: Deadlines for Exemptions and Requests for Exceptions</i> .....	<i>11</i>
	<i>Section 3: Exemption Request and Review Process<sup>1</sup></i> .....	<i>11</i>
	<i>Section 4: Communication concerning which CORE-certified Systems Have Exemptions</i> .....	<i>12</i>
<b>104</b>	<b>Testing Policy</b> .....	<b>13</b>
	<i>Section 1: Key Steps</i> .....	<i>13</i>
<b>105</b>	<b>Enforcement Policy</b> .....	<b>15</b>
	<i>Section 1: Complaint Filing</i> .....	<i>15</i>
	<i>Section 2: For Verified Complaints Only</i> .....	<i>16</i>
	<i>Section 3: For Complaints Not Remedied</i> .....	<i>16</i>
	<i>Section 4: For De-Certified Entities Interested in Re-Certification</i> .....	<i>16</i>
	<i>Request for Review of Possible Non-Compliance Form<sup>1</sup></i> .....	<i>17</i>

### Operating Rules (150-157)

<b>150</b>	<b>Batch Acknowledgements</b> .....	<b>20</b>
	<i>Section 1: Use of the TAI, 997, and 271 Acknowledgments for Batch</i> .....	<i>20</i>
	<i>Section 2: Requirements for Return of TAI or 997</i> .....	<i>20</i>
<b>151</b>	<b>Real Time Acknowledgements</b> .....	<b>22</b>
	<i>Section 1: Use of the TAI, 997, and 271 Acknowledgments for Real Time</i> .....	<i>22</i>
<b>152</b>	<b>Companion Guide Rule</b> .....	<b>24</b>

<sup>1</sup> Please see the CAQH website for access as a stand-alone document.

<sup>2</sup> Please see the CAQH website for specific CORE-certification fees.

## CORE Phase I Eligibility and Benefits Policies and Rules

<b>153</b>	<b>Connectivity Rule.....</b>	<b>37</b>
	<i>Section 1: Usage Patterns.....</i>	<i>37</i>
	<i>Section 2: Real Time Requests.....</i>	<i>37</i>
	<i>Section 3: Batch Submission.....</i>	<i>37</i>
	<i>Section 4: HTTP Data Elements Required and Message Format.....</i>	<i>38</i>
	<i>Section 5: Security and Authentication Requirements.....</i>	<i>38</i>
	<i>Section 6: Response Time, Time Out Parameters and Re-transmission.....</i>	<i>39</i>
	<i>Section 7: Response Message Options and Error Notification.....</i>	<i>39</i>
<b>154</b>	<b>270/271 Data Content Rule .....</b>	<b>41</b>
	<i>Section 1: 270 Eligibility Inquiry.....</i>	<i>41</i>
	<i>Section 2: 271 Eligibility Inquiry Response.....</i>	<i>42</i>
<b>155</b>	<b>Batch Response Time Rule.....</b>	<b>47</b>
	<i>Section 1: 270 Batch Mode Response Time Requirements.....</i>	<i>47</i>
	<i>Section 2: TAI and 997 Batch Mode Response Time Requirements .....</i>	<i>47</i>
	<i>Section 3: Conformance.....</i>	<i>47</i>
<b>156</b>	<b>Real Time Response Time Rule.....</b>	<b>49</b>
	<i>Section 1: 270 Real Time Mode Response Time Requirements .....</i>	<i>49</i>
	<i>Section 2: Conformance.....</i>	<i>49</i>
<b>157</b>	<b>System Availability Rule .....</b>	<b>50</b>
	<i>Section 1: System Availability Requirements.....</i>	<i>50</i>
	<i>Section 2: Reporting Requirements.....</i>	<i>50</i>
	<i>Section 3: Holiday Schedule .....</i>	<i>50</i>

*This document provides the Phase I CORE guiding principles and underlying assumptions that are associated with all Phase I CORE rules.*

**CORE GUIDING PRINCIPLES**

- All CORE Participants and CORE-certified entities will work towards achieving CORE's mission.
- All stakeholders are key to CORE's success; no single organization, nor any one segment of the industry, can do it alone.
- CAQH will strive to include participation by all key stakeholders in the CORE rule making process. CORE has established Governing Procedures; under these Procedures, each CORE member that meets CORE voting criteria will have one vote on CORE issues and rules.
- CAQH serves as the facilitator, while CORE participants draft and vote on the rules.
- Participation in CORE does not commit an organization to adopt the resulting CORE rules.
- Use of and participation in CORE is non-exclusive.
- CORE will not be involved in trading partner relationships, and will not dictate relationships between trading partners.
- To promote interoperability, rules will be built upon HIPAA, and CORE will coordinate with other key industry bodies (for example, X12 and the Blue Cross and Blue Shield Association).
- Where appropriate, CORE will address the emerging interest in XML or other evolving standards.
- Whenever possible, CORE has used existing market research and proven rules. CORE rules reflect lessons learned from other organizations that have addressed similar issues.
- CORE rules will support the Guiding Principles of HHS's National Health Information Network (NHIN).
- CAQH research indicated that there will be benefit to the health care industry as a result of adopting operating rules. CORE will have Measures of Success for Phase I (methodology to measure success and evaluate market impact) and CAQH will report aggregate findings by stakeholder type. Full benefits may not be experienced until Phase II.
- CORE will provide guidance to stakeholders regarding staff implementation and training needs.
- Safeguards will be put in place to make sure that a health plan's benefit and payment information is shared only with the requested provider and is not available to other participating health plans.
- CORE will not build a switch, database, or central repository of information.
- All CORE recommendations and rules will be vendor neutral.
- All of the CORE rules are expected to evolve; Phase I is a starting point and each phase builds upon earlier phases.
- Rules will not be based on the least common denominator but rather will encourage feasible progress.
- CORE will promote and encourage voluntary adoption of the rules.
- CORE participants do not support "phishing."

**UNDERLYING ASSUMPTIONS FOR ALL CORE PHASE I RULES**

- Phase I rules apply only to 270/271 EDI (electronic data interchange) eligibility transactions; DDE (Direct Data Entry) transactions and web-based transactions are not part of the Phase I scope.
- All Phase I rules assume a successful communication connection has been established and that all parties in the transaction routing path are CORE-certified.
- CORE Phase I rules are a floor, not a ceiling; certified entities can go beyond the Phase I rules, e.g. provider accumulator information.
- CORE complies with all antitrust provisions of the law.
- Organizations may sign the Pledge at any time after the CORE rules are developed and approved by the CORE voting members, and may withdraw from the Pledge at any time.
- No individual CORE participant owns the rules or the underlying intellectual property; CAQH/CORE owns the rules and intellectual property.
- The CORE rules will not specify how participants implement any changes to current processes and procedures. CORE will not assume any of the expenses that an organization incurs in making such changes.
- Neither CORE nor participating organizations will be liable if incorrect information is transmitted.
- Complying with CORE rules does not release any organization adopting the rules from ensuring that it is in compliance with all other applicable rules, regulations and legal requirements.
- All organizations that operate under the CORE rules are HIPAA-compliant, and organizations intending to operate under the CORE rules will be asked to attest to this fact. However, CORE will not test for HIPAA compliance.
- CORE rules address both real-time and batch transactions, with movement towards real-time.
- There will not be changes or amendments to the rules unless approved by a CORE vote.

**UNDERLYING PRINCIPLES AND ASSUMPTIONS FOR SPECIFIC RULES****The Pledge**

- Signing the Pledge does not automatically allow the organization to participate in the CORE rule making process; to become involved in the CORE rule making process, the organization must be a CORE participant.
- All stakeholders that sign the Pledge and become CORE-certified stay CORE-certified to maintain their name on the CORE Pledge. There will be a web-based listing of entities that have signed the Pledge.

**Certification**

- There will be a web-based listing of entities that are CORE-certified.

**Enforcement**

- An organization certified under the CORE rules will be party to the CORE enforcement process.

- The CORE enforcement process requires all parties involved in the complaint to be CORE-certified, except for providers that are not CORE-certified but are an end-user of a CORE-certified product.
- CORE-certified entities are permitted to work with any entity of their choice, including entities not participating in CORE.

The Council for Affordable Quality Healthcare (“CAQH”) has created the Committee on Operating Rules for Information Exchange (“CORE”). CORE’s mission is to use common business rules (the “Operating Rules”) to promote interaction of healthcare trading partners and the exchange of healthcare-related information in a consistent, clear, and standardized manner and in compliance with applicable laws and regulations. Developing consistency between trading partners, and thus promoting interoperability, would benefit the healthcare industry by improving the usefulness of healthcare information and reducing administrative costs for stakeholders involved in healthcare data exchange.

Phase I of CORE’s mission is focused on promulgating Operating Rules to increase the usefulness of, and reduce the administrative challenges associated with, eligibility and benefit inquiries by giving providers access to a patient’s eligibility information at the time of service (or before) using the provider’s preferred electronic means. Subsequent phases will broaden the Operating Rules to expand the Operating Rules surrounding eligibility and benefit inquiries and to include additional administrative transaction types consistent with the CORE Vision. As additional Operating Rules are promulgated in subsequent phases, Participant and CORE may incorporate those additional Operating Rules into this Pledge by executing a separate addendum that incorporates the additional Operating Rules into this Pledge.

\_\_\_\_\_ (“Participant”) hereby endorses CORE’s mission.

In furtherance of CORE’s mission, Participant pledges to adopt, implement, and comply with the CORE Operating Rules as promulgated by CORE and in effect as of the date of this Pledge, in accordance with the timeframes set forth in the Operating Rules, *as and to the extent applicable to Participant’s business*. In addition, Participant pledges to use reasonable efforts to encourage Participant’s trading partners to use the CORE Operating Rules. Moreover, Participant will participate in the CORE Certification Program described in the CORE Operating Rules (“Certification”) to the extent applicable.<sup>3</sup> Finally, with the goal of improving the quality and utility of the Operating Rules on an ongoing basis, Participant pledges to provide feedback (which may be either qualitative or quantitative) relating to the Operating Rules.

By signing this Pledge, the Participant also agrees to be publicly recognized as a supporter of CORE’s mission and an endorser of the Phase I Operating Rules. CORE may use Participant’s name and logo (as provided by Participant and subject to any reasonable restrictions around use of the logo provided by the Participant to CORE in writing) solely in connection with such CORE publicity. CORE will make any materials using Participant’s name or logo available to Participant promptly after release and will respond to Participant promptly and in good faith if Participant objects to CORE’s use of Participant’s name or logo. In particular, CORE will discontinue any use of Participant’s name or logo to the extent requested to do so by Participant in writing. Participant, at its option, may participate in the CORE Work Group responsible for designing CORE’s publicity campaign “CORE Marketing Work Group.” Participant may describe itself as an “endorser of the Phase I CORE Operating Rules” or an “endorser of CORE” as long as this Pledge is in effect. Participant may describe itself as “CORE-Certified” only after achieving certification in accordance with the CORE Operating Rules. Participant may not otherwise use the CORE name or marks without CORE’s prior written consent.

---

<sup>3</sup> This clause is meant to address entities that are not subject to Certification (e.g., associations or industry groups) and to address the differences in Certification applicable to different participant-types that are subject to Certification (e.g., providers, payers, vendors, and clearinghouses).

Participant recognizes that the Operating Rules have been developed by a team of representative members of the healthcare industry that have been coordinated by CORE through CAQH and the stakeholders participating in CORE, and Participant agrees that neither CAQH nor CORE (nor their respective members, representatives, and/or agents) will be held responsible for the results of using the Operating Rules in Participant’s business and that neither CAQH nor CORE (or their respective members, representatives, and/or agents) shall have any liability to Participant arising from or related to the Operating Rules or their use by Participant. Remedies for breach of the Operating Rules are as set forth in the Operating Rules; this Pledge does not create any additional remedies against Participant.

Participant recognizes that, as a standard, the Operating Rules are being made publicly available for use by the healthcare industry in anticipation of broad industry adoption. As such, Participant acknowledges that it has no intellectual property rights in the Operating Rules and that any intellectual property rights in the Operating Rules are owned by CAQH on behalf of CORE.

Participant represents that its participation with CORE and this Pledge to use the Operating Rules are entirely voluntary. Participant may withdraw from using the Operating Rules at any time by submitting sixty (60) days written notice to CORE. In addition, CORE (including CORE as acting through CAQH) may terminate this Pledge upon written notice if Participant loses its Certification and such Certification is not reinstated within one-hundred eighty (180) days, or if Participant fails to obtain Certification within one-hundred eighty (180) days of execution of this Pledge. In the event of termination of the Pledge for any reason, Participant must immediately stop using all CORE marks, including any references to being “CORE-certified.”

Accepted:

Acknowledged:

Participant:

Council for Affordable Quality Healthcare  
on behalf of CORE

\_\_\_\_\_

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Robin J. Thomashauer

Title: \_\_\_\_\_

Executive Director

Date: \_\_\_\_\_

Date: \_\_\_\_\_

**GUIDING PRINCIPLES**

- *After signing the CORE Pledge, the entity has 180 days to complete CORE certification testing.*
- *CORE will not certify Phases that CORE has not clearly defined and voted upon.*
- *CORE certification testing will be required by any entity seeking CORE certification. CORE will authorize testing entities to conduct CORE certification testing. All CORE-authorized testing entities will need to be capable of testing for all Phase I rules.*
- *Certification will be available for both real-time and batch processing. However, if an entity does not support batch transactions, it will not be required to comply with the batch rules. An entity that supports both real-time and batch will be required to comply with rules for both. The test scripts allow for the ability to test for both types of processing for each rule.*
- *Upon successful completion of CORE certification testing, CORE entities will receive a CORE certification “Seal” from CAQH.*
- *Entities seeking CORE certification will be required to adopt all of Phase I rules that apply to their business and will be responsible for all their own company-related testing costs.*
- *CORE will not oversee trading partner relationships. CORE-certified entities may work with non-CORE-certified entities if they so desire.*
- *Role of HIPAA compliance:*
  - *It will be assumed by CORE that any covered entity under HIPAA applying for CORE certification will be HIPAA compliant; when submitting testing certification documentation to CORE, covered entities will be asked to sign an attestation form attesting that they are HIPAA compliant to the best of their knowledge (“Attestation Form”) for security, privacy, and the 270/271 transaction. HIPAA compliance will not be defined by CORE.*
- *Role of CORE-authorized testing vendors:*
  - *CORE-authorized testing vendors will be expected to sign the Attestation Form on their own behalf as well, demonstrating that they support a compliant 270/271 transaction.*
- *Who will be certified:*
  - *Certification testing will vary based on participant type. Associations, medical societies and the like will not be certified; instead, these entities will receive a CORE “Endorser” Seal after signing the Pledge. Entities successfully achieving CORE certification will receive the CORE “Seal” that corresponds with their testing application as testing varies by stakeholder type. There will be five different types of CORE “Seals”:*
    - *CORE-certified health plan*
    - *CORE-certified vendor (product specific)*
    - *CORE-certified clearinghouse(product specific)*
    - *CORE-certified provider*
    - *CORE Endorser (for entities that do not create, use, or transmit eligibility information)*
  - *A parent corporation seeking certification will not be certified unless all subsidiaries of the corporation are compliant with CORE rules. Otherwise, each subsidiary of the parent must individually seek certification. For vendors, CORE will apply only to vendor products rather than corporate entities.*

- *Ancillary services are not assumed to be subsidiaries, as a subsidiary is a legal entity of its own that serves as one of the types of key stakeholders that can become certified, e.g., health plan, vendor, or clearinghouse.*
- *If a CORE-certified entity is acquired by an entity that is not CORE-certified, that company will only be allowed to be CORE-certified if the acquired company is the only business that is applicable to the CORE operating rules. If this is not the case, then the newly merged company will be required to seek certification.*
- *Endorsers will not become certified, but will be expected to participate in the CORE public relations campaign, provide CORE feedback and input when requested to do so, and encourage their members to consider participating in CORE.*

## **POLICY**

### **Section 1: Fees**

- Entities seeking CORE certification will be charged two fees: fees related to CORE certification testing as determined by the CORE-authorized certification testing entities and the fee for the CORE Seal as determined by CORE. The goal of CORE is to develop a low-cost certification process in order to support CORE market adoption by small and large entities.

### **Section 2: Period for Which Certification Applies**

- Once certified, CORE-certified entities will remain compliant with applicable CORE rules throughout any system upgrades. When vendors release new versions of their products that affect the functionality of CORE rules, such versions will need to become CORE-certified in order to maintain the CORE Seal.
- Assuming certification is not revoked, CORE certification, except for vendor products, will remain valid until a new version of the CORE rules is established by vote. Revisions will not be made to the rules more than once (1) per year. Revisions to approved rules, if necessary, will become official 20 business days after enacted by CORE. (Version is defined as a substantive change to any approved CORE Phase that requires full CORE membership consent.)

### **Section 3: Key Steps**

The five key steps of CORE certification are presented below:

**Subsection 3.1: Step 1:** Existing entities currently engaged in HIPAA testing will be “authorized” by CORE as CORE-authorized testing entities if they meet certain criteria.

- CORE-authorized testing entities will test entities using the CORE Test Suite.
- CORE will allow any interested entity to apply to CORE to become a CORE-authorized testing entity. However, to become a CORE-authorized testing entity, an interested testing entity must be capable of testing for all Phase I rules and meet a CORE-developed set of criteria. An RFP and beta approval process will identify authorized companies.
- CORE will list any testing entity that is a CORE-authorized testing entity on its website.

**Subsection 3.2: Step 2:** CORE participants seeking certification will work with the CORE-authorized testing entity of their choice to test for CORE compliance.

- Certification testing will differ by role of generator/submitter in the eligibility transaction.

- Any fee/cost imposed by authorized testing entity will be independent and separate from the fee CORE will charge to obtain the CORE Seal. Certification testing fees will be established by each CORE-authorized testing entity; thus prices will be market-driven.
- An authorized CORE testing entity will only provide paperwork to an entity seeking certification after demonstrating successfully their ability to conform with the rules.

**Subsection 3.3: Step 3:** CORE will grant the appropriate CORE Seal after an entity provides all documentation required, including documentation from a CORE-authorized testing entity demonstrating the entity's compliance with CORE rules through successful testing.

- CORE will be responsible for providing the official Seal (after compliance is proven).
- CORE (or its agents) will review test results and maintain a record of CORE-certified entities.
- Applicants will be responsible for ensuring that an authorized person signs the final CORE certification application and the HIPAA attestation, indicating that to the best of the potential participant's knowledge, the applicant is HIPAA compliant for security, privacy, and the 270/271 transaction (or, in the case of a vendor, supports the 270/271 transaction).
  - See attached Attestation form.
- Upon receiving documentation of successful completion of CORE certification testing from an applicant, CORE will have a maximum of 20 business days to respond to the applicant with a clear response of approval or need for clarification. CORE will inform those who apply for certification of the "certification" queue status at the time of their application submission. CORE will complete its assessment within 30 business days unless there are extenuating circumstances. CAQH will report on its website:
  - List of certified entities and endorsers.
  - In the case of vendors and clearinghouses, the CORE-certified transaction(s) processed by their product.
- The fee for the CORE Seal will be based upon a sliding, stakeholder-specific fee scale, similar to the approach of the current CORE membership fee policy.
- The cost of the Seal will be a one-time fee, unlike the CORE participation fee, which is an annual fee. The Seal indicates that an entity/product is CORE-certified, while the CORE participation fee allows entities to participate in the CORE rule writing and voting process. CORE participants may voluntarily decide whether or not to become CORE-certified entities.
- CORE certification will be effective until a new version of the CORE rules is made available, provided an organization has no complaints filed against it, except for vendors, who will be required to seek new CORE certification when a new version of a previously CORE-certified product is released.
- If an entity removes its name from the Pledge, it automatically loses CORE certification.
- When new phases are approved by the CORE membership, re-certification by a CORE-certified entity is not required for an already certified phase.
- As stated in the Pledge, a CORE-certified entity is permitted to market its CORE Seal only if the entity's Seal is valid and current.

**Subsection 3.4: (Potential) Step 4:** Re-certification will be required if an entity's Seal is revoked as a result of a validated complaint of non-compliance. (See enforcement for steps involved in the complaint process.)

- See enforcement process regarding how a validated complaint of non-compliance will be defined and pursued.

**Subsection 3.5: Step 5: Re-certification when CORE rules are modified.**

- Rules will become official 20 business days after being approved by CORE; however, adoption of the rules is not required by participants until 180 business days after signing the Pledge, and a similar timeframe for participant adoption will be added for revisions.
- CORE reserves the right to revise the rules.
- Minor modifications that would improve a rule will not require re-certification.
- Major substantive changes, e.g., new phases, will require re-certification and re-signing of the Pledge relative to the new phase, should the entity choose to pursue certification for the new phase.
- Except for vendors and entities with validated non-compliance, re-certification will be required only after CORE membership approves, by vote, major modifications, changes, or deletions to CORE rules.
- Generally, CORE rules will not be amended between CORE rule phases unless government regulations are issued that impact the rules or as necessary to address problems that arise upon implementation. In this scenario, adoption of the modified rule(s) by CORE participants will be within a reasonable timeframe but will acknowledge/comply with Federal mandates.

**Section 4: Certification Testing Appeals Process**

- Prior to any appeal being submitted, it is assumed efforts have already been taken to try and resolve the issue privately between an entity seeking certification and a CORE-authorized testing vendor, but efforts have not succeeded.
- In the event an entity seeking CORE certification is not satisfied with its testing results, it is permitted to file an appeal of the results to CORE.
- CORE will have 20 business days to investigate the issue. If the appeal is deemed valid, CORE will ask the CORE-authorized testing entity to re-test the results in question within 21 business days of request.
- The Enforcement Committee will have oversight of this process. Please see the CORE 105: Eligibility and Benefits Enforcement Policy version 1.0.1 for more details.

**HIPAA ATTESTATION FORM FOR ENTITIES SEEKING CORE CERTIFICATION**

[ \_\_\_\_\_ ] (“Entity”), in consideration of the Committee on Operating Rules for Information Exchange (“CORE”) deeming Entity eligible to apply to participate in the CORE Certification Program, hereby submits this attestation to compliance with applicable provisions of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the standards promulgated thereunder.

Entity recognizes that CORE does not certify compliance with any aspect of HIPAA or define “HIPAA Compliance.” Entity will not rely on CORE for these determinations.

Entity hereby represents and warrants the following:

- (a) it is, and shall remain, to the best of its knowledge, compliant with standards promulgated by the Secretary of the U.S. Department of Health and Human Services (the “Secretary”) under the Administrative Simplification provisions of Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) that govern health care eligibility benefit inquiry and response, including, as applicable, Parts 160 and 162 of Title 45 of the Code of Federal Regulations, as may be amended from time to time;
- (b) it can send and receive, as applicable or in the case of a software vendor, support the ASC X12N 270/ 271 – Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company (“WPC”), 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, WPC, 004010X092A1, or the current version of such implementation specifications adopted under HIPAA (the “Transaction”);
- (c) it is, and shall remain, to the best of its knowledge, compliant with applicable provisions of the Privacy and Security requirements of Title 45 of the Code of Federal Regulations, Subtitle A, Subchapter C, Parts 160 and 164, as may be amended from time to time.

Entity acknowledges that CORE will rely on this attestation and that any omissions, misrepresentations, or inaccuracies may be a basis for CORE to deny CORE certification.

Entity agrees to notify CORE if it discovers that any of the representations and warranties were not true when made or if it fails to remain compliant with any of the applicable standards set forth above. Entity understands that a loss of compliance with the standards set forth above, or in the case of a software vendor, the ability to support the transaction, may affect CORE certification.

The undersigned representative of Entity affirms that he or she is duly empowered to represent the Entity for purposes of this attestation and has knowledge confirming the accuracy of this attestation.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Position

\_\_\_\_\_  
Date

## **BACKGROUND**

*This rule addresses certification exemptions that health plans seeking CORE certification may request when the health plan has a scheduled migration of an existing IT system(s) if the remainder of the health plan's IT systems are CORE compliant. This rule is complementary and does not replace the following CORE policies, which are already part of the CORE 102: Eligibility and Benefits Certification Policy version 1.0.1.*

- *Entities may seek certification for their subsidiaries versus their corporate entity. The CORE certification Seal will apply to the subsidiary or the corporation, whichever entity seeks CORE certification.*
- *If a CORE-certified entity is acquired by an entity that is not CORE-certified, that company will only be allowed to be CORE-certified if the acquired company is the only business that is applicable to the CORE operating rules. If this is not the case, then the newly merged company will be required to seek certification.*

## **POLICY**

### **Section 1: Required Criteria to be Granted a CORE Health Plan IT System Exemption:**

Any health plan seeking an IT System Certification Exemption must meet the following criteria or gain approval from the CORE Steering Committee for an exception:

#### **Subsection 1.1: Membership Percentage**

Percentage of a health plan's full membership eligibility data that is processed by the IT system(s) in question:

- No more than 30 percent of a health plan's total membership can be processed by the IT system(s) to be covered by the exemption.

#### **Subsection 1.2: Timing**

Time period for which the IT system(s) in question must be scheduled for migration:

- Migration must be scheduled for completion no later than 12 months from the date of when the health plan is granted CORE certification.
- If migration is not completed within the agreed-upon 12 months from the date of CORE certification, the health plan could be de-certified (see below).

### **Section 2: Deadlines for exemptions and requests for exceptions**

- IT system exemptions *and exceptions* will be reviewed and granted on an individual health plan basis as decided by the CORE Steering Committee.
- Exemptions that are due to newly acquired entities will only be granted if the same above parameters on time periods and percentage of membership are met.
- Approving exceptions will be the responsibility of the CORE Steering Committee.

### **Section 3: Exemption Request and Review Process**

#### **Subsection 3.1: Exemption Request**

Any health plan seeking an exemption must follow the CORE Certification Policy, excluding the IT system(s) for which they are seeking the exemption.

- When providing CAQH with the documentation to prove successful CORE certification testing and attest to HIPAA compliance, the health plan must provide CAQH with an executive-level attestation stating that the health plan meets the agreed-upon IT system exemption criteria and has the ability to identify those transactions to which the exemption applies. As a result, CORE will be able to accurately respond to those Requests for Review of Possible Non-Compliance that are the result of IT system exemptions.
- If possible, the plan will communicate to CAQH, in a way that is most meaningful to the market/providers, the systems/groups/products for which Phase I eligibility data will not be available until after the exemption time period expires.
- If the proper CORE certification documentation is received, CAQH will be responsible for granting exemptions just as it is responsible for granting CORE Seals.
- The 12-month IT system exemption period will begin on the day that the health plan is granted CORE certification (a CORE Seal) by CAQH.

### **Subsection 3.2: Review Process**

On or before the last business day of the month in which exemption ends, the health plan must communicate to CORE that the migration is/is not complete.

- It is the goal of the CORE Steering Committee to build momentum for CORE certification and this goal will be taken into consideration when reviewing requests for *exceptions* to the exemption policy.
- If a certified health plan with an exemption communicates to CORE that the IT system migration was not completed in the agreed-upon timeframe, the CORE Steering Committee will determine how to address the issue.
- Decisions by the CORE Steering Committee to remove the CORE Seal, or to provide an exception shall be conducted within 20 business days. Decisions by the Steering Committee shall be final.
- If de-certified, the health plan will need to reapply for CORE certification.
- The CORE Enforcement Policy outlines the steps to become re-certified after being de-certified. Health plans wanting to become re-certified due to non-compliance with an IT exemption rule will need to be re-certified for all CORE Phase I transactions.

### **Section 4: Communication Concerning Which CORE-certified Systems Have Exemptions**

- In Phase I, all CORE-certified entities will be listed on the CAQH website (see CORE 102: Eligibility and Benefits Certification Policy version 1.0.1).
- There will be an asterisk (\*) next to those certified health plans that have an IT system exemption. The asterisk will indicate that a portion of the plan's membership systems are not CORE compliant; detailed information identifying those systems/groups/products specific to each plan will be provided, if available.
- The asterisk will only be removed when the health plan communicates to CAQH that its exempted system(s) are in compliance.

**GUIDING PRINCIPLES**

- *The CORE testing policy will be used to gain CORE certification only; it does not outline trading partner implementation interoperability testing activities.*
- *Third parties that have become CORE-authorized certification testing entities through a standard CORE evaluation process will be used by interested parties to test for CORE rules compliance. CORE will authorize any testing entity that meets CORE's testing entity criteria. A key criteria in becoming a CORE-authorized testing entity will be that the entity is capable of testing for all Phase I rules.*
- *A prerequisite for obtaining a stakeholder-specific CORE-certified Seal will be the successful completion of a stakeholder-specific CORE Test Suite, which will be demonstrated through proper documentation from a CORE-authorized testing entity.*
- *All parties essential to the success of the eligibility transaction will be addressed in the CORE certification testing process: providers, health plans, clearinghouses, and vendors. CORE testing will vary by stakeholder type, e.g., provider, health plan, clearinghouses, vendors. Associations, medical societies and the like will not undergo certification testing as they are endorsers of CORE rather than certified entities.*
- *The CORE testing protocol will be scoped only to demonstrate conformance with CORE rules, and not overall compliance with HIPAA; however, each entity submitting an application for CORE certification will sign a statement affirming that it is HIPAA compliant to the best of its knowledge.*

**POLICY****Section 1: Key Steps****Subsection 1.1: Step 1: CORE pre-certification, self-testing**

- To prepare for certification, entities seeking CORE certification can review rules and conduct internal testing as they see appropriate.

**Subsection 1.2: Step 2: CORE certification processing testing**

- A CORE-authorized certification testing vendor performs testing with an entity seeking CORE certification based upon CORE Phase I testing criteria specific to the participant's stakeholder type.
- Entities seeking CORE certification can work with the CORE-authorized testing entity of their choice to test and/or use a testing website developed by one or more of the companies to conduct their CORE Phase I testing. If website approach is taken, individual company testing results would not be shared publicly. The CORE Test Suite includes scenario-based testing and expected outcomes.
- CORE Test Suite focuses on current industry eligibility 'pain points' and therefore includes testing for all of the Phase I CORE rules, including the following:

CORE Rule	Key Aspect of CORE Stakeholder-Specific Testing <sup>1</sup>			
	Providers	Health Plans	Vendors	Clearinghouses
Connectivity Rule	Yes	Yes	Yes	Yes
Response Time Rule: Batch and Real Time	Yes <sup>2</sup>	Yes <sup>2</sup>	Yes <sup>2</sup>	Yes <sup>2</sup>
270/271 Data Content Rule	Yes	Yes	Yes	Yes
Acknowledgements Rule: Batch and Real Time	Yes	Yes	Yes	Yes
Companion Guide	Yes	Yes	Yes	Yes
System Availability	Yes	Yes	Yes	Yes

**Subsection 1.3: Step 3:** CORE-authorized testing vendor verifies, with documentation, that an entity seeking CORE certification has successfully completed testing; participant can apply to CORE to obtain the CORE Seal by sending documentation to CORE. (Certification Process begins, please see CORE 102: Eligibility and Benefits Certification Policy version 1.0.1.)

**Subsection 1.4: Step 4:** Certification Testing Appeals Process

- Prior to any appeal being submitted, it is assumed efforts have already been taken to try and resolve the issue privately between an entity seeking certification and a CORE-authorized testing vendor, but efforts have not succeeded.
- In the event an entity seeking CORE certification is not satisfied with its testing results, it will be permitted to file a written appeal of the results to CORE, under the guidance of the Enforcement Committee (please see CORE 105: Eligibility and Benefits Enforcement Policy version 1.0.1.)
- CORE will have 20 business days to investigate the issue. If the appeal is deemed valid, CORE will ask the CORE-authorized testing entity to re-test the results in question within 21 business days of request.

<sup>1</sup> Entities will be tested under the stakeholder-specific test bed for which they want to receive CORE certification, e.g. health plan gets tested on health plan test bed in order to receive CORE Health Plan Seal.

<sup>2</sup> Certification in Phase I is not exhaustive. For example, as part of certification testing, these stakeholders will need to demonstrate their ability to capture response time statistics. The actual delivery of such statistics by a CORE-certified entity will only be required in response to a verified compliance complaint.

**GUIDING PRINCIPLES**

- *CORE participants will be encouraged to privately resolve disputes before submitting a formal complaint of non-compliance against a CORE-certified entity.*
- *Enforcement will be a complaint-driven process that will require documentation (electronic or paper) demonstrating multiple instances of non-compliance.*
- *Any healthcare provider that is an end-user of a CORE-certified product/service may lodge a complaint against a CORE-certified entity. Beyond end-users, only an organization that is CORE-certified and involved in the alleged non-compliant transactions may file a complaint.*
- *The details of a specific complaint will remain confidential. Names or other identifying information will not be publicly released. This information will only be used and disclosed by CORE for its non-compliance review. If an entity is found to be in actual violation of a CORE rule(s), its certification will be terminated and its name removed from the CORE website if the complaint is not remedied per the CORE enforcement timeline.*
- *The complaint process will be progressive, but will last no more than six (6) months between filing of complaint and resolution. Extensions may be granted on a case-by-case basis due to mitigating factors decided upon by the Enforcement Committee.*
- *The Enforcement Committee will consist of a balance of stakeholder types from the CORE membership (certified health plans, vendors, PMS, provider vendors, clearinghouses, and providers). No one stakeholder type will be permitted to have a dominant representation.*
- *Entities are permitted to withdraw a complaint at any time during the complaint process.*
- *Personal health information (PHI) must not be submitted without appropriate authorization.*
- *CORE will accept and review any submitted complaint that contains the required documentation.*

**POLICY****Section 1: Complaint Filing**

Every effort must be made to resolve problems before a complaint is filed. Conformance language for each rule should assist entities with what is required of CORE-certified entities.

**Subsection 1.1: Step 1:** Complaint formally filed with CORE, including proper documentation.

- Includes a completed CORE-developed form, Request for Review of Possible Non-Compliance, that outlines the violation, and at least five documented examples of the violation(s) over a 30-day period, demonstrating that the violation was not a one-time occurrence but occurred in multiple instances.
- Organization filing complaint must do so within 90 days of the most recent compliance violation(s) for which it is being filed.

**Subsection 1.2: Step 2:** CORE, under the guidance of the Enforcement Committee, reviews complaint form for completeness and timeliness, and verifies/dismisses complaint.

- Information gathered from entity filing complaint.
- Organization in question given an opportunity to respond to complaint in writing.
- CORE must respond to the complaint within 20 business days.
- All organizations involved in the complaint must respond to requests for information by CORE within 20 business days. The complaint must be deemed valid or invalid within

30 business days after all documentation is reviewed by CORE and requests for information are received.

*(Process ends if inquiry dismissed. If inquiry verified, process continues.)*

**Section 2: For Verified Complaints Only**

**Subsection 2.1: Step 1:** Entities found to be out of compliance with a CORE rule(s) will be informed by CORE that they have a defined grace period (40 business days) in order to remedy the problem by successfully re-testing for compliance with the rule(s) or be de-certified.

- An Enforcement Committee composed of objective participants will review verified complaints, and will be responsible for providing any extension to this grace period.
- Enforcement Committee terms will be limited to one year from date of appointment.
- Conflicts of interest will be avoided on a case-specific basis at the request of the entity being reviewed for non-compliance. If a member of the Enforcement Committee is party to a complaint, then he/she will recuse him/herself for the duration of the resolution of the complaint.
- The membership of the Enforcement Committee will be appointed by the Steering Committee from nominations made by Steering Committee members and/or CORE members. Until there is an equal representation of stakeholders, or until a sufficient number of certified entities exist, Subgroup and/or Work Group Chairs will serve on the Enforcement Committee.
- 10 business days after the grace period, entities will prove they have remedied the problem by presenting to the Enforcement Committee documentation of at least five instances on five different business days over a span of 10 business days in which there was no issue of compliance with the entity that filed the complaint, in addition to providing documentation of successful re-testing.
- The Enforcement Committee will be responsible for granting variances to the 40 business day grace period.

**Section 3: For Complaints not Remedied**

**Subsection 3.1: Step 1:** De-certification/removal of CORE Seal.

**Section 4: For De-Certified Entities Interested in Re-Certification**

**Subsection 4.1: Step 1:** A de-certified entity may seek re-certification; entities are responsible for all fees associated with re-certification, including any fees for a new Seal.

- Entities seeking re-certification due to non-compliance will only need to do so for the rule with respect to which they were found to be non-compliant. CORE-authorized testing companies will provide documentation on the entity's compliance with the rule specific to the applicable CORE Test Suite.

**Request for Review of Possible Non-Compliance Form**

**PREREQUISITES**

- 1) Entity filing complaint must be party to the transaction and with the exception of providers, CORE-certified. Any healthcare provider that is an end-user of a CORE-certified product/service may lodge a complaint against a CORE-certified entity.
- 2) Entities being filed against must be CORE-certified.
- 3) Filing this form assumes reasonable steps have already been taken by your company to try and resolve the issue privately with your trading partner, but such efforts were not successful.
- 4) At least five documented examples of the violation(s) over a 30-day period must be provided with this form.
- 5) Entity must file a complaint within 90 days of the most recent compliance violation(s) for which it is being filed.
- 6) The details of a specific complaint remain private. Names or other identifying information will not be publicly released. This information will only be used and disclosed by CORE for its non-compliance review. If an entity is found to be in actual violation of a CORE rule(s), its certification will be terminated and its name removed from the CORE website if the complaint is not remedied per the CORE enforcement timeline.
- 7) Entities are permitted to withdraw a complaint any time during the complaint process.

**If you have any questions about this form, contact CAQH at: (202) 861-6380 or CORE@caqh.org**

<b>CORE: Non-Compliance Complaint Form</b>			
<b>Please provide your contact information (All fields required.)</b>			
<b>Organization Name and Type (Health Plan, Provider, Clearinghouse, Vendor)</b>			
<b>Name (First and Last)</b>			
<b>Street Address</b>	<b>City/Town</b>	<b>State</b>	<b>Zip</b>
<b>Telephone Number</b>		<b>Email Address</b>	
<b>Organization filing complaint against (All fields required.)</b>			
<b>Organization Name and Type (Health Plan, Provider, Clearinghouse, Vendor)</b>			
<b>Name (First and Last)</b>			

<b>CORE: Non-Compliance Complaint Form</b>			
<b>Street Address</b>	<b>City/Town</b>	<b>State</b>	<b>Zip</b>
<b>Telephone Number</b>		<b>Email Address</b>	
<p><b>When did this alleged violation occur? mm/dd/yyyy (Required field)</b></p> <p>1.</p> <p>2.</p> <p>3.</p> <p>4.</p> <p>5.</p>			
<p><b>Have efforts been made to address the problem? Who at the company in question have you been working with to resolve the issue?</b></p>			
<p><b>Identify the rule complaint category.</b> (Required field.) Select one category listed below per complaint submission. Complete this form again to file a complaint for another category.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Response Time</li> <li><input type="checkbox"/> System Availability</li> <li><input type="checkbox"/> Service Type and Benefit Summary</li> <li><input type="checkbox"/> Patient Financial Responsibility</li> <li><input type="checkbox"/> Acknowledgements</li> <li><input type="checkbox"/> Connectivity Safe Harbor</li> <li><input type="checkbox"/> Companion Guide</li> </ul>			

<b>CORE: Non-Compliance Complaint Form</b>	
<b>Describe, in detail, the alleged violation.</b> (Required field.) You may attach/upload additional pages as needed. Please enclose at least five examples of your complaint.	
<b>Please sign and date this complaint. (Required field)</b>	
<b>SIGNATURE:</b>	<b>DATE:</b>

**SUBMISSION PROCESS**

Filing a complaint with CORE is voluntary. However, without the information required on the Non-Compliance Complaint Form, CORE may not be able to proceed with a complaint. Names or other identifying information will remain private unless an entity is found to be in actual violation of a CORE rule(s), and then their certification will be terminated and their name removed from the CORE website if the complaint is not remedied per the CORE enforcement timeline.

To submit a complaint electronically please:

- Send as an attachment by email to CORE@caqh.org;
- Submit by fax 202-861-1454;
- Mail to:  
 CAQH re: CORE Compliance Review  
 601 Pennsylvania Ave, NW  
 South Building, Suite 500  
 Washington, DC 20004.

Note: All signatures must be hand-written. Electronic signatures will not be accepted.

**NEXT STEPS**

*See CORE 105: Eligibility and Benefits Enforcement Policy version 1.0.1. Section 2.*

## **BACKGROUND**

*This rule for use of acknowledgements for batch mode places parallel responsibilities on both submitters of the 270 inquiries (providers) and submitters of the 271 responses (health plans or information sources) for sending and accepting TA1 and 997 acknowledgements. The goal of this approach is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate health plan correction of errors in their outbound responses.*

*The rule assumes a successful communication connection has been established and that all parties in the transaction routing path are CORE-certified.*

## **RULE**

### **Section 1: Use of the TA1, 997, and 271 Acknowledgements for Batch**

#### **Subsection 1.1: Reporting on a Batch 270 or 271 Submission that is Rejected**

##### *ISA Interchange Rejection*

The TA1 Interchange Acknowledgement is used only to indicate a rejection (negative acknowledgement) of the ISA/IEA Interchange containing the 270 batch inquiries or 271 batch responses. The receiver of the batch (provider, clearinghouse, intermediary, health plan or information source) must always return the TA1 in the case of an ISA/IEA rejection, regardless of the value in the ISA 14-I13 Acknowledgement Requested indicator.

##### *Functional Group or Transaction Set Rejection*

If the 270 batch inquiries or 271 batch responses pass ISA/IEA editing, but an X12 standards syntax error resulting in a rejection is found during the validation of the Functional Group(s) or Transaction Set(s) within a Functional Group, the receiver of the batch (the provider, clearinghouse, intermediary, health plan or information source) must always return a 997 Functional Acknowledgement to indicate a rejection (negative acknowledgement).

#### **Subsection 1.2: Reporting on Batch Envelope that is Accepted**

The receiver of the batch (provider, clearinghouse, intermediary, health plan or information source) must always return a 997 Functional Acknowledgement if the 270 or 271 batch complies with all X12 standard syntax requirements (positive acknowledgement) to indicate that the batch has been accepted for processing. Therefore, in batch mode, the receiver (provider, clearinghouse, intermediary, health plan or information source) will always return a 997 acknowledgement indicating either rejection or acceptance of the batch.

If the 270 batch is accepted for processing, a batch of 271 responses are subsequently returned to the submitter by the health plan (or information source.) The AAA segments in the 271 responses are used to report business level error situations.

### **Section 2: Requirements for Return of TA1 or 997**

The TA1 Interchange Acknowledgement or the 997 Functional Acknowledgement must not be returned during the initial communications session in which the 270 batch is submitted. Reference the CORE 153 Eligibility and Benefit Connectivity and CORE 155 Online Eligibility and Benefit Batch Response Time (Section 2: TA1 and 997 Response Time Requirements) rules for the timing and availability of these two acknowledgements.

**CONFORMANCE**

*Conformance with this rule is considered achieved by receivers of the batch (provider, clearinghouse, intermediary, health plan or information source) if all of the following criteria are achieved:*

1. *A TAI is returned only to indicate an Interchange error resulting in the rejection of the entire Interchange; the ISA 14-I13 Acknowledgement Requested field is ignored.*
  - a) *A TAI must not be returned if there are no errors in the Interchange control segments.*
2. *A 997 is returned to indicate either acceptance of a Functional Group (including the enclosed Transaction Set) or to indicate a Functional Group or the enclosed Transaction Set error resulting in the rejection of the entire Functional Group.*
  - a) *A 997 must always be returned even if there are no errors in the Functional Group and enclosed Transaction Set.*
3. *A 271 eligibility response transaction must always be returned for an Interchange, Functional Group and Transaction Set that complies with X12 standard syntax requirements.*
  - a) *A 271 eligibility response transaction may contain either the appropriate AAA Validation Request segment(s) in the case of a business level error or the data segments containing the requested eligibility and benefit status details.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

## **BACKGROUND**

*Rule assumes a successful communication connection has been established and that all parties in the transaction routing path are CORE-certified.*

*This CORE Phase I rule addresses only acknowledgements for receivers of the 270 for Real Time. It does not address acknowledgements that receivers of the 271 must consider.*

## **RULE**

### **Section 1: Use of the TA1, 997, and 271 Acknowledgements for Real Time**

#### **Subsection 1.1: Reporting on a Real-Time 270 Submission that is Rejected**

##### *ISA/IEA Interchange Rejection*

The TA1 Interchange Acknowledgement will be used only to indicate a rejection (negative acknowledgement) of the ISA/IEA Interchange containing the 270 Eligibility Benefit Inquiry Request. The receiver of the 270 request (clearinghouse, intermediary, health plan or information source) must always return the TA1 in the case of an ISA/IEA rejection, regardless of the value in the ISA 14-I13 Acknowledgement Requested indicator.

##### *Functional Group or Transaction Set Rejection*

If the 270 passes ISA/IEA editing, but an error is found during the validation of the Functional Group(s) or Transaction Set(s) within a Functional Group, the receiver of the 270 request (clearinghouse, intermediary, health plan or information source) must always return a 997 Functional Acknowledgement to indicate a rejection (negative acknowledgement). If there are no errors, a 997 must not be returned.

#### **Subsection 1.2: Reporting on a Real time 270 Submission that is Accepted**

If the 270 complies with the X12 standard syntax requirements, then the 271 Eligibility Inquiry Response will be returned to the submitter.

The AAA segments in the 271 will be used to report business level error situations.

#### **Subsection 1.3: Summary**

Therefore the submitter of a 270 in real-time will receive only one acknowledgement/response from the receiver (clearinghouse, intermediary, health plan or information source): a TA1 (error); a 997 (error); or a 271.

## **CONFORMANCE**

*Conformance with this rule is considered achieved by receivers of the 270 request (clearinghouse, intermediary, health plan or information source) if all of the following criteria are achieved:*

1. *A TA1 is returned only to indicate an Interchange error resulting in the rejection of the entire Interchange; the ISA 14-I13 Acknowledgement Requested field is ignored.*
  - a) *A TA1 must not be returned if there are no errors in the Interchange control segments.*
2. *A 997 is returned only to indicate a Functional Group (including the enclosed Transaction Set) error resulting in the rejection of the entire Functional Group.*

**CORE 151: Eligibility and Benefit Real Time Acknowledgement Rule version 1.0.0**

- a) *A 997 must not be returned if there are no errors in the Functional Group and enclosed Transaction Set.*
- 3. *A 271 eligibility response transaction must always be returned for an Interchange, Functional Group and Transaction Set that complies with X12 standard syntax requirements.*
  - a) *A 271 eligibility response transaction may contain either the appropriate AAA Validation Request segment(s) in the case of a business level error or the data segments containing the requested eligibility and benefit status details.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

**BACKGROUND**

*Health plans or information sources have the option of creating a "companion guide" that describes the specifics of how they will implement the HIPAA transactions. The companion guide is in addition to and supplements the X12 Implementation Document, adopted for use under HIPAA.*

*Currently health plans or information sources have independently created companion guides that vary in format and structure. Such variance can be confusing to trading partners/providers who must review numerous companion guides along with the X12N Implementation Documents. To address this issue, CORE developed this 270/271 Companion Guide Template for health plans or information sources. Using this template, health plans or information sources can ensure that the structure of their companion guide is similar to other health plan's documents, making it easier for providers to find information quickly as they consult each health plan's document on these important industry EDI transactions.*

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

*Although CORE participants believe that a standard template/common structure is desirable, they recognize that different health plans may have different requirements. The CORE Companion Guide template gives health plans the flexibility to tailor the document to meet their particular needs.*

*Note: This Companion Guide template has been adapted from the CAQH/WEDI Best Practices Companion Guide Template originally published January 1, 2003.*

**RULE**

All CORE-certified entities' Companion Guides covering the 270/271 eligibility inquiry and response transactions must follow the format/flow as defined in the CORE 270/271 Companion Guide Template for HIPAA Transactions. (See template for details.)

Note: This rule does not require any CORE-certified entity to modify any other existing companion guides that cover other HIPAA-adopted transaction implementation guides.

**CONFORMANCE**

*Conformance with this rule is considered achieved by health plans (or information sources) if all of the following criteria are achieved:*

- 1. Publication to its trading partner community of its detailed companion guide specifying all requirements for submitting and processing the 270 eligibility transaction and returning the 271 eligibility inquiry response transaction in accordance with this rule.*
- 2. Submission to an authorized CORE certification testing company the following:*
  - a) A copy of the table of contents of its official 270/271 companion guide.*
  - b) A copy of a page of its official 270/271 companion guide depicting its conformance with the format for specifying the 270/271 data content requirements.*

**CORE 152: Eligibility and Benefit Real Time Companion Guide Rule version 1.0.0**

- c) *Such submission may be in the form of a hard copy paper document, an electronic document, or a URL where the table of contents and an example of the 270/271 content requirements of the companion guide is located.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

---

**Acme Health Plan**

HIPAA Transaction  
Standard Companion Guide

**Refers to the Implementation Guides Based on X12 version 004010A1**

**Companion Guide Version Number: 1.1**

**October 2005**

**Disclosure Statement**

This document ...

**2005 © Acme Health Plan**

All rights reserved. This document may be copied.

**Preface**

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

**EDITOR'S NOTE:**

This page is blank because major sections of a book should begin on a right hand page.

**Table of Contents**

1 Introduction .....6

    1.1 Scope .....7

    1.2 Overview .....7

    1.3 References .....7

    1.4 Additional Information .....7

2 Getting Started .....7

    2.1 Working with Acme Health Plan .....7

    2.2 Trading Partner Registration.....7

    2.3 Certification and Testing Overview.....7

3 Testing with the Payer .....7

4 Connectivity with the Payer / Communications .....7

    4.1 Process flows .....7

    4.2 Transmission Administrative Procedures .....7

        4.2.1 Re-transmission procedures .....7

    4.3 Communication protocol specifications .....8

    4.4 Passwords .....8

5 Contact information .....8

    5.1 EDI Customer Service .....8

    5.2 EDI Technical Assistance .....8

    5.3 Provider Service Number .....8

    5.4 Applicable websites / e-mail.....8

6 Control Segments / Envelopes .....8

    6.1 ISA-IEA .....8

    6.2 GS-GE .....8

    6.3 ST-SE .....8

7 Payer Specific Business Rules and Limitations .....8

    7.1 CORE Level of Certification .....8

8 Acknowledgements and/or Reports.....9

    8.1 Report Inventory .....9

9 Trading Partner Agreements .....9

    9.1 Trading Partners .....9

10 Transaction Specific Information .....9

## 1 INTRODUCTION

This section describes how X12N Implementation Guides (IGs) adopted under HIPAA will be detailed with the use of a table. The tables contain a row for each segment that Acme Health Plan has something additional, over and above, the information in the IGs. That information can:

1. Limit the repeat of loops, or segments
2. Limit the length of a simple data element
3. Specify a sub-set of the IGs internal code listings
4. Clarify the use of loops, segments, composite and simple data elements
5. Any other information tied directly to a loop, segment, composite or simple data element pertinent to trading electronically with Acme Health Plan

In addition to the row for each segment, one or more additional rows are used to describe Acme Health Plan's usage for composite and simple data elements and for any other information. Notes and comments should be placed at the deepest level of detail. For example, a note about a code value should be placed on a row specifically for that code value, not in a general note about the segment.

The following table specifies the columns and suggested use of the rows for the detailed description of the transaction set companion guides.

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
193	2100C	NM1	Subscriber Name			This type of row always exists to indicate that a new segment has begun. It is always shaded at 10% and notes or comment about the segment itself goes in this cell.
195	2100C	NM109	Subscriber Primary Identifier		15	This type of row exists to limit the length of the specified data element.
196	2100C	REF	Subscriber Additional Identification			
197	2100C	REF01	Reference Identification Qualifier	18, 49, 6P, HJ, N6		These are the only codes transmitted by Acme Health Plan.
			Plan Network Identification Number	N6		This type of row exists when a note for a particular code value is required. For example, this note may say that value N6 is the default. Not populating the first 3 columns makes it clear that the code value belongs to the row immediately above it
218	2110C	EB	Subscriber Eligibility or Benefit Information			
231	2110C	EB13-1	Product/Service ID Qualifier	AD		This row illustrates how to indicate a component data element in the Reference column and also how to specify that only one code value is applicable.

#### **SCOPE**

This section specifies the appropriate and recommended use of the Companion Guide.

#### **OVERVIEW**

This section specifies how to use the various sections of the document in combination with each other.

#### **REFERENCES**

This section specifies additional documents useful for the read. For example, the X12N Implementation Guides adopted under HIPAA that this document is a companion to.

#### **ADDITIONAL INFORMATION**

This section, completed by the payer, includes other information useful to the reader. For example:

- Assumptions regarding the reader
- Advantages / benefits of EDI

## **2 GETTING STARTED**

#### **WORKING WITH ACME HEALTH PLAN**

This section describes how to interact with Acme Health Plan's EDI Department.

#### **TRADING PARTNER REGISTRATION**

This section describes how to register as a trading partner with Acme Health Plan.

#### **CERTIFICATION AND TESTING OVERVIEW**

This section provides a general overview of what to expect during any certification and testing phases.

## **3 TESTING WITH THE PAYER**

This section contains a detailed description of the testing phase.

## **4 CONNECTIVITY WITH THE PAYER / COMMUNICATIONS**

#### **PROCESS FLOWS**

This section contains process flow diagrams and appropriate text.

#### **TRANSMISSION ADMINISTRATIVE PROCEDURES**

This section provides Acme Health Plan's specific transmission administrative procedures.

#### **RE-TRANSMISSION PROCEDURE**

This section provides Acme Health Plan's specific procedures for re-transmissions.

#### **COMMUNICATION PROTOCOL SPECIFICATIONS**

This section describes Acme Health Plan's communication protocol(s).

#### **PASSWORDS**

This section describes Acme Health Plan's use of passwords.

### **5 CONTACT INFORMATION**

#### **EDI CUSTOMER SERVICE**

This section contains detailed information concerning EDI Customer Service, especially contact numbers.

#### **EDI TECHNICAL ASSISTANCE**

This section contains detailed information concerning EDI Technical Assistance, especially contact numbers.

#### **PROVIDER SERVICE NUMBER**

This section contains detailed information concerning the payment of claims, especially contact numbers.

#### **APPLICABLE WEBSITES / E-MAIL**

This section contains detailed information about useful web sites and email addresses.

### **6 CONTROL SEGMENTS / ENVELOPES**

#### **ISA-IEA**

This section describes Acme Health Plan's use of the interchange control segments. It includes a description of expected sender and receiver codes, authorization information, and delimiters.

#### **GS-GE**

This section describes Acme Health Plan's use of the functional group control segments. It includes a description of expected application sender and receiver codes. Also included in this section is a description concerning how Acme Health Plan expects functional groups to be sent and how Acme Health Plan will send functional groups. These discussions will describe how similar transaction sets will be packaged and Acme Health Plan's use of functional group control numbers.

#### **ST-SE**

This section describes Acme Health Plan's use of transaction set control numbers.

### **7 PAYER SPECIFIC BUSINESS RULES AND LIMITATIONS**

This section describes Acme Health Plan's business rules, for example:

1. Billing for specific services such as DME, Ambulance, Home Health
2. Communicating payer specific edits
3. CORE Level of Certification

## **8 ACKNOWLEDGEMENTS AND OR REPORTS**

This section contains information and examples on any applicable payer acknowledgements

### **REPORT INVENTORY**

This section contains a listing/inventory of all applicable acknowledgement reports

## **9 TRADING PARTNER AGREEMENTS**

This section contains general information concerning Trading Partner Agreements (TPA). An actual TPA may optionally be included in an appendix.

### **TRADING PARTNERS**

An EDI Trading Partner is defined as any Acme customer (provider, billing service, software vendor, employer group, financial institution, etc.) that transmits to, or receives electronic data from Acme.

Payers have EDI Trading Partner Agreements that accompany the standard implementation guide to ensure the integrity of the electronic transaction process. The Trading Partner Agreement is related to the electronic exchange of information, whether the agreement is an entity or a part of a larger agreement, between each party to the agreement.

For example, a Trading Partner Agreement may specify among other things, the roles and responsibilities of each party to the agreement in conducting standard transactions.

## **10 TRANSACTION SPECIFIC INFORMATION**

This section describes how X12N Implementation Guides (IGs) adopted under HIPAA will be detailed with the use of a table. The tables contain a row for each segment that Acme Health Plan has something additional, over and above, the information in the IGs. That information can:

1. Limit the repeat of loops, or segments
2. Limit the length of a simple data element
3. Specify a sub-set of the IGs internal code listings
4. Clarify the use of loops, segments, composite and simple data elements
5. Any other information tied directly to a loop, segment, composite or simple data element pertinent to trading electronically with Acme Health Plan

In addition to the row for each segment, one or more additional rows are used to describe Acme Health Plan's usage for composite and simple data elements and for any other information. Notes and comments should be placed at the deepest level of detail. For example, a note about a code value should be placed on a row specifically for that code value, not in a general note about the segment.

The following table specifies the columns and suggested use of the rows for the detailed description of the transaction set companion guides.

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
193	2100C	NM1	Subscriber Name			This type of row always exists to indicate that a new segment has begun. It is always shaded at 10% and notes or comment about the segment itself goes in this cell.
195	2100C	NM109	Subscriber Primary Identifier		15	This type of row exists to limit the length of the specified data element.
196	2100C	REF	Subscriber Additional Identification			
197	2100C	REF01	Reference Identification Qualifier	18, 49, 6P, HJ, N6		These are the only codes transmitted by Acme Health Plan.
			Plan Network Identification Number	N6		This type of row exists when a note for a particular code value is required. For example, this note may say that value N6 is the default. Not populating the first 3 columns makes it clear that the code value belongs to the row immediately above it
218	2110C	EB	Subscriber Eligibility or Benefit Information			
231	2110C	EB13-1	Product/Service ID Qualifier	AD		This row illustrates how to indicate a component data element in the Reference column and also how to specify that only one code value is applicable.

## **Appendices**

This section contains one or more appendices.

### **1. Implementation Checklist**

This appendix contains all necessary steps for going live with Acme Health Plan.

### **2. Business Scenarios**

This appendix contains free format text descriptions of typical business scenarios. The transmission examples for these scenarios are included in Appendix C.

### **3. Transmission Examples**

This appendix contains actual data streams linked to the business scenarios from Appendix B.

### **4. Frequently Asked Questions**

This appendix contains a compilation of questions and answers relative to Acme Health Plan and its providers. Typical question would involve a discussion about code sets and their effective dates.

### **5. Change Summary**

This section describes the differences between the current Companion Guide and previous guide(s).

## **BACKGROUND**

*This rule addresses proposed usage patterns for both batch and real time transactions, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message exchanges beyond declaring that the HIPAA-mandated X12 formats must be used between covered entities and security information must be sent outside of the X12 payload.*

*This rule is designed to provide a “safe harbor” that application vendors, providers, and health plans (or other information sources) can be assured will be supported by any CORE-certified trading partner. All CORE-certified organizations must demonstrate the ability to implement connectivity as described in this rule. This rule is not intended to require trading partners to remove existing connections that do not match the rule, nor is it intended to require that all CORE trading partners must use this method for all new connections. CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than that described by this rule.*

*This rule describes some of the specifics for implementing HTTP/S connectivity for healthcare administrative transaction exchange.*

## **RULE**

CORE-certified entities must be able to implement HTTP/S Version 1.1 over the public Internet as a transport method for the eligibility inquiry and response transactions (270/271). Information Sources must be able to perform the role of an HTTP/S server, while Information Receivers must be able to perform the role of an HTTP/S client. HTTP/S is a secure, reliable, ubiquitous protocol that has a proven record of support for high-volume transaction exchange and security in healthcare and other industries. In addition, there is wide system-developer and software tools support for HTTP/S, making it a relatively inexpensive transport for information sources and receivers to support.

### **Section 1: Usage Patterns**

HTTP/S supports a request-response message pattern, meaning that the sender submits a message and then waits for a response from the message receiver. This works well for the submission of both batch and real time X12 messages, but the response message from the receiver is different depending on whether the sender’s message is a real time request, batch submission, or batch request pickup.

### **Section 2: Real Time Requests**

Real time requests must include a single inquiry or submission (e.g. one eligibility inquiry to one information source for one patient). In this model the response from the message receiver is either an error response (see below for error reporting) or the corresponding X12 message response (e.g. a TA1, 997 or 271 if the request was a 270).

### **Section 3: Batch Submission**

Batch requests are sent in the same way as real time requests. In this model the response will differ because message receivers are not required to provide an X12 response in the timeframes specified by CORE for real time. For batch submissions, the response must be only the standard HTTP message indicating whether the request was accepted or rejected (see below for error reporting.) Message receivers must not respond to a batch submission with an X12 response such as a TA1 or 997 as described in the CORE 150: Eligibility and Benefits Batch Acknowledgement Rule version 1.0.0 in the HTTP response to the batch request, even if their systems’ capabilities

allow such a response. (See the CORE 155: Batch Response Time Rule version 1.0.0 for the response time requirements for TA1 or 997.)

For full details of the standard HTTP messages, see [RFC 2616](#).<sup>1</sup> In general a 2xx series response means that the batch submission has been accepted for further processing, while a 4xx or 5xx series response means that the submission has not been accepted and will not be processed by the message receiver.

### **Subsection 3.1: Batch Response Pickup**

Batch responses should be picked up after the message receiver has had a chance to process a batch submission (see the CORE 155: Batch Response Time Rule version 1.0.0 for details on timing). Under this usage pattern, the message sender connects to the message receiver using HTTP/S and sends a message requesting available files, and responder then sends back either.

- 1) The file(s) in the HTTP/S response message (payload), or
- 2) A list of available file(s), and supports a mechanism to request a particular file from the list.

## **Section 4: HTTP Data Elements Required and Message Format**

### **Subsection 4.1: Required Data Elements**

Certain business data elements: authorization information, a payload identifier, and date and time stamps, must be included in the HTTP message body outside of the X12 data. Information Sources must publish their detailed specification for the message format in their publicly available Companion Guide.

In order to comply with the CORE 155 and 156: Response Time Rules version 1.0.0, message receivers will be required to track the times of any received inbound messages, and respond with the outbound message for that payload ID. In addition, message senders must include the date and time the message was sent in the HTTP Message Header tags.

### **Subsection 4.2: Date and Time Requirements**

This Phase I rule does not define the exact format and attributes for these data elements except that the date must be sent and logged using 8 digits (YYYYMMDD) and time must be sent and logged using a minimum of 6 digits (HHMMSS).

*This Rule does not address issues of Batch Response Integrity; those are addressed by the CORE 150 Batch Acknowledgements Rules version 1.0.0.*

## **Section 5: Security and Authentication Requirements**

By using the HTTP/S protocol, all information exchanged between the sender and receiver is encrypted by a session-level private key negotiated at connection time. This approach makes it very difficult for an intruder to decode the encrypted data.

### **Subsection 5.1: User ID and Password**

CORE participants will employ User ID and Password as the default minimum criteria authentication mechanism. Issuance, maintenance and control of password requirements may vary by participant and should be issued in accordance with the organizations' HIPAA Security Compliance policies. CORE recommends that the User ID and Password policies and requirements be published in each password issuer's Companion Guide.

---

<sup>1</sup> The Internet Society. Network Work Group. <http://www.ietf.org/rfc/rfc2616.txt>. June 1999.

The User ID and Password authentication must be encrypted by the HTTP/S protocol, but passed outside of the X12 payload information as described in the HTTP Message format section. This allows message receivers to authenticate that the message is from a trusted source before passing it to their X12 parsing engine.

The receiver may also require the message sender to register the IP address for the host or subnet originating the transaction, and may refuse to process transactions whose source is not registered or does not correspond to the ID used.

Due to programming requirements of POSTing over HTTP/S, use of a digital certificate is required to establish communications. CORE-certified participants will make available information on how to obtain the receiver's root public certificate.

No additional security for file transmissions, such as the separate encryption of the X12 payload data, is required in this Phase I CORE Rule for connectivity. By mutual consent, organizations can implement additional encryption, but HTTP/S provides sufficient security to protect healthcare data as it travels the Internet.

### **Section 6: Response Time, Time Out Parameters and Re-transmission**

*This section of the rule relates to connectivity and telecommunications response times and time outs. The CORE 150 and 151 Batch and Real Time Acknowledgements Rules version 1.0.0 describe the responsibilities of CORE participants in responding to business messages (e.g. the X12 270) with the appropriate business response (e.g. the X12 TA1, 997, 271, etc).*

If the HTTP Post Reply Message is not received within the 60 second response period, the provider's system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

If no response is received after the second attempt, the provider's system should submit no more than 5 duplicate transactions within the next 15 minutes.

If the additional attempts result in the same timeout termination, the provider's system should notify the provider to contact the health plan or information source directly to determine if system availability problems exist or if there are known Internet traffic constraints causing the delay.

### **Section 7: Response Message Options and Error Notification**

*This section of the rule addresses only the HTTP Post Message responses. Please refer to CORE 150 and 151 Eligibility and Benefits Acknowledgement Rules version 1.0.0 for required acknowledgments.*

The HTTP Post Message process requires a response (or "reply") to the message that was sent. The response sent back from the message receiver (e.g. the various information sources) can fall into several different categories depending on the type of the request and the capabilities of the message receiver.

#### **Subsection 7.1: Authorization Errors**

If the username and/or password included in the request are not valid according to the message receiver, the message receiver must send back an HTTP 403 Forbidden error response with no data content.

#### **Subsection 7.2: Batch Submission Acknowledgement**

At the message acknowledgement level, a message receiver must send back a response with a status code of HTTP 202 Accepted once the message has been received. This does not imply that the X12 content has been validated or approved.

**Subsection 7.3: Real Time Response or Response to Batch Response Pickup**

When a message receiver is responding to a real time request or a batch response pickup request, assuming that the message authorization passed, the receiver must respond with an HTTP 200 Ok status code and the X12 data content as specified by the CORE 150 and 151 Batch and Real Time Acknowledgements Rules version 1.0.0.

**Subsection 7.4: Server Errors**

It is possible that the HTTP server is not able to process a real time or batch request. In this case, the message receiver must respond with a standard HTTP 5xx series error such as HTTP 500 Internal Server Error or HTTP 503 Service Unavailable. If a sender receives a response with this error code, they will need to resubmit the request at a later time, because this indicates that the message receiver will never process this message.

**CONFORMANCE**

*Conformance with this connectivity rule is considered achieved by information sources if all of the following criteria are achieved:*

- 1. The Information Source must publish their detailed HTTP Message format specification in a publicly available Companion Guide.*
- 2. The Information Source must demonstrate the ability to respond in their production environment to valid and invalid logon/connection requests with the appropriate HTTP errors as described in the Response Message Options & Error Notification section of this rule.*
- 3. The Information Source must demonstrate the ability to log, audit, track and report the required data elements as described in the HTTP Message Format section of this rule.*
- 4. The Information Source's HTTP/S-based connectivity method must be available for use by submitters for 95 percent of the information source's documented system availability as specified in the CORE System Availability rule and measured over a calendar month. Each CORE-certified entity must demonstrate its conformance with this criterion by demonstrating their ability to track and report the times the HTTP/S-based connectivity system was available.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

**BACKGROUND**

*This CORE rule specifies the CORE minimum requirements for using the HIPAA-adopted 270 Eligibility Inquiry to inquire about health plan insurance coverage and to respond to such an inquiry using the HIPAA-adopted 271 Eligibility Response implementation guide. This CORE rule covers the following content in the 270 inquiry and 271 response:*

1. *The required response to a inquiry when the individual is located in the health plan's system under the following conditions:*
  - a) *A generic 270 inquiry*
  - b) *A specific inquiry for a Service Type not supported by the health plan*
  - c) *A specific inquiry for one of the CORE required service types*
2. *The mandated response components include:*
  - a) *the status of eligibility (active, inactive, etc.) for both the health plan and benefits*
  - b) *the dates of eligibility at the health plan (contract) level for past, current and future dates and the dates of eligibility at the benefit level if different from the contract level*
  - c) *the patient financial responsibility for each specified benefit at the base contract amounts for both in-network and out-of-network*
  - d) *the name of the health plan*

*The requirements specified in this CORE rule address certain situational elements and codes and are in addition to requirements contained in the HIPAA-adopted 270/271 implementation guides.*

**RULE****Section 1: 270 Eligibility Inquiry<sup>7</sup>****Subsection 1.1: HIPAA Requirements**

As specified in the HIPAA-adopted 270/271 Eligibility Inquiry implementation guide, a health plan (or information source) must support a generic request for eligibility. This is accomplished by the submission of service type Code "30" (Health Benefit Plan Coverage) in the "EQ" loops of the transaction.

Providers may also send inquiries for specific service type, identified by codes specified in the HIPAA Implementation Guide.

When a health plan (or information source) receives a generic request for eligibility or if the health plan (or information source) does not support the specific service type as indicated by the code submitted, and the individual is located in the system, the health plan must respond in the 271 as specified below in this CORE rule.

The HIPAA-adopted 270 Eligibility Inquiry implementation guide allows providers to submit an inquiry for three types of eligibility dates in the loops 2100C, 2110C, 2100D, and 2110D:

- code "307" Eligibility
- code "435" Admission
- code "472" Service

---

<sup>7</sup> The language of the proposed CORE rule is adapted from the draft version 5010 270/271 guide currently being developed.

**Subsection 1.2: CORE Requirements**

This CORE rule will further constrain these dates as specified herein. A date submitted in either the 2100C or 2100D loops is considered to apply globally to all of the service types specified in the EQ segment.

- When the 270 is a generic request for eligibility and a date is submitted in either or both of the 2100C or 2100D loops, all CORE-certified participants are required to submit only code “307” Eligibility.
- The use of code “307” in either loop 2100C or 2100D means the submitter is requesting the health plan (or information source) to respond with the date on which the health plan coverage begins.

A date submitted in either the 2110C or 2110D loop is considered to apply only to the benefit begin service date for the service type specified by each EQ01-1365 service type code. When a date is submitted in either or both of the 2110C or 2110D loops, all CORE-certified participants are required to submit only code “307” Eligibility.

- When code “307” is used in either loop 2110C or 2110D it means the submitter is requesting the health plan (or information source) to respond in the corresponding 2110C or 2110D loops in the 271 with the date on which the benefit eligibility covering the individual begins only if the benefit begin date is different from the plan begin date specified in either the 2100C or 2100D loops.

**Section 2: 271 Eligibility Inquiry Response**<sup>8,9</sup>

The HIPAA Implementation Guide for the 270/271 Eligibility Inquiry implementation guide states: *“An information source must respond with either an acknowledgment that the individual has active or inactive coverage or that the individual was not found in their system.”* The CORE rule for the 271 response imposes these additional requirements: If the individual is located in the health plan’s (or information source’s) system, the following must be returned:

**Subsection 2.1: Status**

The status of the benefit in EB01-1390 using codes 1 through 8 (active through inactive status) or I (Non-covered) and using Code “30” in EB03-1365 as appropriate for the health plan covering the individual in either the 2110C or 2110D loop.

**Subsection 2.2: Health Plan Name**

The health plan name (if one exists within the health plan’s or information source’s system) in EB05-1204 Plan Coverage Description. Neither the health plan or information source is required to obtain such a health plan name from outside its own organization.

---

<sup>8</sup> The language of the CORE rule is adapted from the draft version 5010 270/271 guide currently being developed.

<sup>9</sup> This CORE rule is not intended to be a comprehensive companion document specifying the complete content of either the 270 Eligibility Inquiry or 271 Eligibility Response transaction sets. The focus on this CORE rule is on specifications for the 271 Eligibility Response to address the CORE Phase I data requirements for benefit coverage.

**Subsection 2.3: Patient Financial Responsibility**

The patient financial responsibility for co-insurance, co-payment and deductibles must be returned as specified below by a CORE-certified health plan (or information source) for each of the service type codes returned:<sup>10</sup>

**Subsection 2.3.1: To specify the co-insurance responsibility**

Use code “A” Co-Insurance in EB01-1390 Eligibility or Benefit Information data element and use EB08-954 Percent data element for each reported type of service. The percent amount expressed is the portion that is the patient’s responsibility. Negative numbers are prohibited. *Please refer to Subsection 2.5: Support Required for Generic Request for further detail.*

1. When the patient’s portion of responsibility for a benefit is nothing, place zero (0) in data element EB08-954 and return this segment.
2. When co-insurance does not apply to a benefit, do not return this segment. If the patient financial responsibility amounts differ for in and out of network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as appropriate.
3. The health plan (or information source) may, at its discretion, elect not to return co-insurance information for the following services specified in EB03-1365: 1 – Medical Care; 30 – Health Plan Benefit Coverage; 35 – Dental Care; 88 – Pharmacy; AL – Vision (Optometry). This optional reporting does not preempt the health plan’s (or information source’s) requirement to report patient co-payment responsibility for the remaining 5 CORE required service types (33 – Chiropractic, 48 – Hospital Inpatient, 50 – Hospital Outpatient, 86 – Emergency Services, 98 – Professional (Physician) Visit – Office) that must be reported in a generic request for eligibility (Service Type Code 30) or a service type not supported by the health plan. This requirement is outlined in subsection 2.5 below.

**Subsection 2.3.2: To specify the co-payment responsibility**

Use code “B” Co-Payment in EB01-1390 Eligibility or Benefit Information data element and use EB07-782 Monetary Amount element for each reported type of service. The dollar amount expressed is the portion that is the patient’s responsibility. Negative numbers are prohibited. *Please refer to Subsection 2.5: Support Required for Generic Request for further detail.*

1. When the patient’s portion of responsibility for a benefit is zero dollars, place zero (0) in data element EB07-782 and return this segment.
2. When a co-payment does not apply to a benefit, do not return this segment. If the patient financial responsibility amounts differ for in and out of network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as appropriate.

---

<sup>10</sup> This CORE rule is not intended to be a comprehensive companion document specifying the complete content of either the 270 Eligibility Inquiry or 271 Eligibility Response transaction sets. The focus on this CORE rule is on specifications for the 271 Eligibility Response to address the CORE Phase I data requirements for patient financial responsibility.

3. The health plan (or information source) may, at its discretion, elect not to return co-payment information for the following services specified in EB03-1365: 1 – Medical Care; 30 – Health Plan Benefit Coverage; 35 – Dental Care; 88 – Pharmacy; AL – Vision (Optometry). This optional reporting does not preempt the health plan’s (or information source’s) requirement to report patient co-payment responsibility for the remaining 5 CORE required service types (33 – Chiropractic, 48 – Hospital Inpatient, 50 – Hospital Outpatient, 86 – Emergency Services, 98 – Professional (Physician) Visit – Office) that must be reported in a generic request for eligibility (Service Type Code 30) or a service type not supported by the health plan. This requirement is outlined in subsection 2.5 below.

#### **Subsection 2.3.3: To specify the deductible responsibility**

Use code “C” Deductible in EB01-1390 Eligibility or Benefit Information data element and use EB07-782 Monetary Amount to indicate the dollar amount of the deductible for the type of service specified in EB03-1365 service type code. The dollar amount expressed is the portion that is the patient’s responsibility. Negative numbers are prohibited. *Please refer to Subsection 2.5: Support Required for Generic Request for further detail.*

1. When the patient’s portion of responsibility for a benefit is zero dollars, place zero (0) in data element EB07-782 and return this segment.
2. When a deductible does not apply to a benefit, do not return this segment. If the patient financial responsibility amounts differ for in and out of network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as appropriate.
3. If the deductible amount varies by the benefit coverage level specified in EB02-1207 Coverage Level Code, place the appropriate code in EB02 and use additional occurrences of the EB Eligibility or Benefit Information segment as necessary for each benefit coverage level for each type of service, e.g., individual or family coverage.
4. The health plan (or information source) may, at its discretion, elect not to return deductible information for the following services specified in EB03-1365: 1 – Medical Care; 30 – Health Plan Benefit Coverage; 35 – Dental Care; 88 – Pharmacy; AL – Vision (Optometry). This optional reporting does not preempt the health plan’s (or information source’s) requirement to report patient deductible responsibility for the remaining 5 CORE required service types (33 – Chiropractic, 48 – Hospital Inpatient, 50 – Hospital Outpatient, 86 – Emergency Services, 98 – Professional (Physician) Visit – Office) that must be reported in a generic request for eligibility (Service Type Code 30) or a service type not supported by the health plan. This requirement is outlined in subsection 2.5 below.

#### **Subsection 2.4: Eligibility Dates**

If the individual has active coverage (codes 1 through 5 in EB01-1390), the code “307” Eligibility date (defined to mean health plan begin in the context of this CORE rule) must be returned in the DTP segment in either the 2100C or 2100D loops. The health plan or information source may alternately return a range of dates if known using code RD8 in DTP02-1250 Date Time Period Format Qualifier data element.

1. If the benefit begin dates are different from the health plan begin dates specified in the 2100C or 2100D loops, then code “348” Benefit Begin date must be returned in either the 2110C or 2110D loop with the associated EB03 benefit.

2. The response will be as of the date the transaction is processed as specified in the 271 BHT04 Transaction Set Creation Date, unless a specific date (prior, current or future) was used from the DTP segment in either the 2100C or 2100D loops of the 270 eligibility inquiry.

3. The 270 eligibility inquiry may request a benefit coverage date 12 months in the past or up to the end of the current month. If the inquiry is outside of this date range and the health plan (or information source) does not support eligibility inquiries outside of this date range, the 271 response must include the AAA segment with code “62” Date of Service Not Within Allowable Inquiry Period in the AAA03-901 Reject Reason Code data element.

**Subsection 2.5: Support Required for Generic Request or Service Code not Supported.**

If the 270 submitted is a generic request for eligibility (service type code "30" in the "EQ" loops of the transaction), or a request for a service type not supported by the health plan (or information source), the following CORE service type code values must be returned in EB03-1365 service type code in either the 2110C or 2110D loops:

<b>CORE REQUIRED SERVICE TYPES</b>	
<b>CORE REQUIRED SERVICE TYPES (X12 270/271 Code Definition)<sup>11</sup></b>	<b>CORE DESCRIPTION</b>
1 – Medical Care	Medical care services to diagnose and/or treat medical condition, illness or injury. Medical services and supplies provided by physicians and other health care professionals.
30 – Health Benefit Plan Coverage	---
33 – Chiropractic	Professional services which may include office visits, manipulations, lab, x-rays, and supplies.
35 – Dental Care	Benefits for services, supplies or appliances for care of teeth.
48 – Hospital Inpatient	Hospital services and supplies for a patient who has been admitted to a hospital for the purpose of receiving medical care or other health services.
50 – Hospital Outpatient	Hospital services and supplies for a patient who has not been admitted to a hospital for the purpose of receiving medical care or other health services.
86 – Emergency Services	Medical services and supplies provided by physicians, Hospitals, and other healthcare professionals for the treatment of a sudden and unexpected medical condition or injury which requires immediate medical attention.
88 – Pharmacy	Drugs and supplies dispensed by a licensed Pharmacist, which may include mail order or internet dispensary.
98 – Professional (Physician) Visit - Office	Professional services of a Physician or other Health Care Professional during an office visit.
AL – Vision (Optometry)	Routine vision services furnished by an optometrist. May include coverage for eyeglasses, contact lenses, routine eye exams, and/or vision testing for the prescribing or fitting of eyeglasses or contact lenses.

<sup>11</sup> CORE descriptions (clarification/meaning) are meant to provide a general understanding of the specific services which are included in each service type, but may not be all inclusive.

1. If the individual has active coverage and any of the above codes are not a covered benefit, then code "I" Not Covered must be returned in the EB01.
2. If the health plan's (or information source's) plan benefits do not fall into any of the service type codes listed above, except service type code "30", the health plan must return the Active Status information as specified in Subsection 2.1 of this rule and whatever additional appropriate service type code does define the benefit.
3. If no specific service type code exists, the health plan may return the appropriate procedure code(s) in EB13 or a description MSG01. EB03 and EB13 cannot both be used in the same EB segment.

#### **Subsection 2.6: Support for CORE Required Service Types**

The health plan (or information source) must support an explicit request for each of the CORE service types. The corresponding service type codes are: "1", "33", "35", "48", "50", "86", "88", "98", or "AL" submitted in the 270 EQ01 by providing the content identified in subsections 2.1 through 2.4 above for the submitted service type(s).

#### **Subsection 2.7: Support for Other Service Type Codes**

Additional covered service type codes may be returned at the health plan's (or information source's) discretion; however their absence does not imply that they are not covered.

### **CONFORMANCE**

*The CORE test suite for this rule includes the following types of tests:*

1. *Receipt by a health plan or information source of a valid generic request for eligibility 270 transaction created using the CORE master test bed data.*
2. *The creation of an eligibility response 271 transaction generated using the CORE master test bed data.*
  - a) *The CORE master test bed data will contain all of the values necessary to generate a response transaction covering each of the requirements in the following paragraphs of the 271 Eligibility Inquiry Response section of this rule:*
    - i) *Subsection 2.2: health plan name*
    - ii) *Subsection 2.4: health plan begin date*
    - iii) *Subsection 2.4.(1): benefit begin date*
    - iv) *Sections 2.1 and 2.5: benefit coverage (service types) status, covered/non-covered benefits*
    - v) *Subsection 2.3: patient financial responsibility for co-insurance, co-payment, and deductible, including in-network and out-of-network*

*The CORE test suite will not include comprehensive testing requirements to test for all possible permutations of health plan benefit status or patient financial responsibility for all of the CORE required benefits addressed in the 271 response.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

## **BACKGROUND**

*When 270 eligibility inquiries submitted in batch processing mode are subsequently converted to real-time processing by any intermediary clearinghouse or switch for further processing by the health plan (or information source) before being returned to the submitter as a batch of 271 responses, the CORE 155: Eligibility and Benefits Batch Response Time Rule version 1.0.0 shall apply.*

## **RULE**

### **Section 1: 270 Batch Mode Response Time Requirements**

Maximum response time when processing in batch mode<sup>1</sup> for the receipt of a 271 response to a 270 inquiry submitted by a provider or on a provider's behalf by a clearinghouse/switch by 9:00pm Eastern time of a business day must be returned by 7:00am Eastern time the following business day. A business day consists of the 24 hours commencing with 12:00am (Midnight or 0000 hours) of each designated day through 11:59pm (2359 hours) of that same designated day. The actual calendar day(s) constituting business days are defined by and at the discretion of each health plan or information source. *See CORE 157: System Availability Rule version 1.0.0 for notification process of holidays.*

### **Section 2: TA1 and 997 Batch Mode Response Time Requirements**

TA1 or 997 responses must be available to the submitter within one hour of receipt of the batch: to the provider in the case of a batch of 270 inquiries and to the health plan (or information source) in the case of a batch of 271 responses.<sup>2</sup>

### **Section 3: Conformance**

Conformance with this maximum response time rule shall be considered achieved if 90 percent of all required responses as specified in the CORE 150: Eligibility and Benefit Batch Acknowledgement Rule version 1.0.0 are returned within the specified maximum response time as measured within a calendar month.

Each CORE-certified entity must demonstrate its conformance with this maximum response time rule by demonstrating its ability to capture, log, audit, match and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

## **CONFORMANCE**

*The CORE test suite for this rule includes the following:*

- 1. The actual delivery of statistics by a CORE-certified entity will be required only in response to a verified compliance complaint. Otherwise, a CORE-certified entity's compliance with the response time requirements will be based on good faith. Please see CORE 105: Eligibility and Benefits Enforcement Policy version 1.0.1 for details on filing complaints and who is permitted to file complaints.*

---

<sup>1</sup> Batch mode is defined in the CORE Glossary of Terms

<sup>2</sup> See CORE 150: Batch Acknowledgements Rule version 1.0.0, which requires return of either a TA1 to be sent only to indicate a rejection, and a 997 to be sent in all cases indicating rejection/acceptance of the batch.

2. *All CORE-certified entities are required to conform to this rule regardless of the connectivity mode and methods used between CORE-certified trading partners.*
3. *This rule assumes that all parties in the transaction routing path are CORE-certified and compliant.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

**RULE**

**Section 1: 270 Real Time Mode Response Time Requirements**

Maximum response time when processing in real time mode<sup>1</sup> for the receipt of a 271 (or in the case of an error, a TA1 or 997) response from the time of submission of a 270 inquiry must be 20 seconds (or less). TA1 and 997 response errors must be returned within the same response timeframe.<sup>2</sup> See *CORE 157: System Availability Rule version 1.0.0 for notification process of holidays*.

**Section 2: Conformance**

Conformance with this maximum response time rule shall be considered achieved if 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each CORE-certified entity must demonstrate its conformance with this maximum response time rule by demonstrating its ability to capture, log, audit, match and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

**CONFORMANCE**

*The CORE test suite for this rule includes the following:*

- 1. The actual delivery of statistics by a CORE-certified entity will be required only in response to a verified compliance complaint. Otherwise, a CORE-certified entity's compliance with the response time requirements will be based on good faith.*
- 2. All CORE-certified entities are required to conform to this and other CORE rules regardless of the connectivity mode and methods used between CORE-certified trading partners.*
- 3. This rule assumes that all parties in the transaction routing path are CORE-certified and compliant.*
- 4. The recommended maximum response time between each participant in the transaction is 4 seconds or less per hop as long as the 20-second total roundtrip requirement is met.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*

---

<sup>1</sup> Real-time mode is defined in the CORE Glossary of Terms.

<sup>2</sup> See CORE 151: Real Time Acknowledgements Rule version 1.0.0, which requires return of either a TA1, 997, or 271 response.

**BACKGROUND**

*Many healthcare providers have a need to determine an individual's health plan coverage at the time and point of patient registration and intake, which may occur on a 24x7x365 basis or outside of the typical business day and business hours. Additionally, many institutional providers are now allocating staff resources to performing patient pre-registration activities on weekends and evenings. As a result, providers have a business need to be able to conduct health plan eligibility transactions at any time.*

*On the other hand, health plans have a business need to take their eligibility and other systems offline periodically in order to perform the required system maintenance. This typically results in some systems not being available for timely eligibility inquiries and responses certain nights and weekends. The rule was created to address these conflicting needs.*

**RULE****Section 1: System Availability Requirements**

System availability<sup>1</sup> must be no less than 86 percent per calendar week<sup>2</sup> for both real-time and batch processing modes. This will allow for health plan, (or other information source) clearinghouse/switch or other intermediary system updates to take place within a maximum of 24 hours per calendar week for regularly scheduled downtime.

**Section 2: Reporting Requirements****Subsection 2.1: Scheduled Downtime**

CORE-certified health plans (or information sources), clearinghouses/switches or other intermediaries must publish their regularly scheduled system downtime in an appropriate manner (e.g., on websites or in companion guides) such that the healthcare provider can determine the health plan's system availability so that staffing levels can be effectively managed.

**Subsection 2.2: Non-Routine Downtime**

For non-routine downtime (e.g., system upgrade), an information source must publish the schedule of non-routine downtime at least one week in advance.

**Subsection 2.3: Unscheduled Downtime**

For unscheduled/emergency downtime (e.g., system crash), an information source will be required to provide information within one hour of realizing downtime will be needed.

**Subsection 2.4: No Response Required**

No response is required during scheduled downtime(s.)

**Section 3: Holiday Schedule**

Each health plan, (or other information source) clearinghouse/switch or other intermediary will establish its own holiday schedule and publish it in accordance with the rule above.

---

<sup>1</sup> System is defined as all necessary components required to process a 270 inquiry and return response.

<sup>2</sup> Calendar week is defined as 12:01am Sunday to 12:00am the following Sunday.

**CONFORMANCE**

*Each CORE-certified entity must demonstrate its conformance with this system availability rule by publishing the following documentation:*

- 1. Actual published copies of regularly scheduled downtime schedule, including holidays, and method(s) of publishing.*
- 2. Sample of non-routine downtime notice and method(s) of publishing.*
- 3. Sample of unscheduled/emergency downtime notice and method(s) of publishing.*

*Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.*