simplifying healthcare administration
CAQH

CORE™
Committee on Operating Rules for Information Exchange
A CAQH Initiative

CORE Phase II Policies and Operating Rules

Approved July 2008
v5010 Update March 2011

CORE Phase II Policies (200-205)

CORE Phase II Operating Rules (250, 258-260, 270)

Phase II Glossary of Data Content Terms: http://www.caqh.org/pdf/CLEAN5010/PIIGlossary.pdf

Phase II Certification Test Suite: http://www.caqh.org/pdf/CLEAN5010/COREPIITestSuite-v5010.pdf

Phase II CORE 200 Guiding Principles
version 2.1.0 March 2011

This document provides the Phase II CORE guiding principles and underlying assumptions that are associated with all Phase II CORE Operating 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 Phase II CORE Operating 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-adopted standards, and CORE will coordinate with other key industry bodies (for example, ASC X12 and the Blue Cross 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 Operating 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 II (methodology to measure success and evaluate market impact) and CAQH will report aggregate findings by stakeholder type.
- 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 Operating Rules are expected to evolve; Phase I was 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 PHASE II CORE OPERATING RULES

- Phase II CORE Operating Rules apply to ASC X12 005010X279A1 Eligibility and Benefit Request and Response (270/271) Technical Report Type 3 (hereafter v5010 270/271*)* and ASC X12 005010X212 Health Care Claim Status Request and Response (276/277) Technical Report Type 3 (hereafter v5010 276/277*)* implementation guides; DDE (Direct Data Entry) transactions and web-based transactions are not part of the Phase II scope.
- All Phase II CORE Operating Rules assume a successful communication connection has been established and that all parties in the transaction routing path are CORE-certified.
- Phase II CORE Operating Rules are a floor, not a ceiling; certified entities can go beyond the Phase II CORE Operating Rules, e.g., real time response time less than 10 seconds.
- CORE complies with all antitrust provisions of the law.
- Organizations may sign the Pledge at any time after the Phase II CORE Operating 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 Phase II CORE Operating 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 Phase II CORE Operating 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 Phase II CORE Operating Rules are HIPAA-compliant, and organizations intending to operate under the Phase II CORE Operating Rules will be asked to attest to this fact. However, CORE will not test for HIPAA compliance.
- Phase II CORE Operating 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 Operating Rule making process; to become involved in the CORE Operating Rule making process, the organization must be a CORE participant.
- All stakeholders that sign the Pledge and become CORE-certified must 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.
- A separate signed Pledge Addendum is required for Phase II.

Certification

- There will be a web-based listing of entities that are CORE-certified.
- Vendors and clearinghouses need only certify for the transaction type(s) offered (i.e. eligibility and/or claim status)

Enforcement

- An organization certified under the CORE Operating 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.

CORE® Phase II Pledge

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 II of CORE's mission is focused on promulgating CORE 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 CORE Operating Rules to expand the CORE Operating Rules surrounding eligibility and benefit inquiries and to include additional administrative transaction types consistent with the CORE Vision. As additional CORE Operating Rules are promulgated in subsequent phases, Participant and CORE may incorporate those additional CORE Operating Rules into this Pledge by executing a separate addendum that incorporates the additional CORE 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 CORE 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.[3] Finally, with the goal of improving the quality and utility of the CORE Operating Rules on an ongoing basis, Participant pledges to provide feedback (which may be either qualitative or quantitative) relating to the CORE 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 II 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 II CORE Operating Rules" or an "endorser of CORE" as long as this Pledge is in effect. Participant may describe itself as Phase II "CORE-certified" only after achieving certification in accordance with the Phase II CORE Operating Rules. Participant may not otherwise use the CORE name or trademarks without CORE's prior written consent.

Participant recognizes that the CORE 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 CORE 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 CORE Operating Rules or their use by Participant. Remedies for breach of the CORE Operating Rules are as set forth in the CORE Operating Rules; this Pledge does not create any additional remedies against Participant.

[3] 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).

Phase II CORE 201 Pledge
version 2.1.0 March 2011

Participant recognizes that the CORE 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 CORE Operating Rules and that any intellectual property rights in the CORE Operating Rules are owned by CAQH on behalf of CORE.

Participant represents that its participation with CORE and this Pledge to use the CORE Operating Rules are entirely voluntary. Participant may withdraw from using the CORE 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: _____

For Phase II Certification or Endorsement: Refer to the following page for Phase II Addendum.

Phase II CORE Pledge Addendum

This addendum to the Phase I CORE Pledge supplements the Phase I CORE Pledge (the "Pledge") signed by CAQH and Participant, and extends Participant's support of the Committee on Operating Rules for Information Exchange ("CORE") to Phase II CORE. In particular, CAQH has promulgated Phase II of CORE ("CORE Phase II") to build upon the Phase I Eligibility and Benefits (270/271) related Phase I CORE Operating Rules updated to support v5010 of the HIPAA-adopted ASC X12 Technical Report Type 3 implementation guides, and add operating rules updated to support v5010 of the ASC X12 005010X212 Health Care Claim Status Request and Response (276/277) transaction. Participant hereby extends its support of CORE in the Pledge to include support of Phase II. Subject to the extension to Phase II as set forth in this addendum, the provisions of the Pledge shall continue to apply to Phase I CORE without change.

Accepted:	Acknowledged:
Participant:	Council for Affordable Quality Healthcare
_____	on behalf of CORE
By: _____	By: _____
Name: _____	Robin J. Thomashauer
Title: _____	Executive Director
Date: _____	Date: _____

Phase II CORE® Seal Application
version 2.1.0 March 2011

A. Contact Information

_____
Organization

_____
Name of product being certified *(if applicable)*

_____
Contact Name *(individual responsible for your organization's CORE-certification process)*

_____
Mailing Address

_____
Phone

_____
Fax

_____
Email

B. Required Documents (Please attach the following with this application)

Certifiers

1. Certification testing results documentation (as provided by the CORE-authorized certification testing vendor with which you worked).
2. HIPAA attestation form (requires executive-level signature).
3. Health Plan IT exemption request (if applicable; requires executive-level signature).
4. Signed Pledge (Unless previously submitted)

Endorsers

1. Signed Pledge

C. Phase II CORE Certification and Endorsement Terms and Conditions

1. An entity's Seal will be revoked as a result of a validated complaint of non-compliance (see Phase II CORE 205 Enforcement Policy for more information).
2. Certification is required for each Phase of CORE rules.
3. Re-certification and re-endorsement is required for each substantive change made to Phase II CORE and additional Phase rules. Substantive changes will occur no more than once per year.
4. To health plans granted an exemption, the 12-month IT system exemption period will begin on the day that the health plan is granted its CORE Seal.
5. After receiving a Phase II CORE Seal, the entity may market itself as a CORE Endorser or CORE-Certified.

D. CAQH CORE Responsibilities

1. CORE will notify you of your "certification" queue status at the time CORE receives your application.
2. CORE will complete its assessment within 30 business days unless there are extenuating circumstances.
3. CORE will grant your stakeholder-specific CORE Seal following review and approval of its application.
4. Entities receiving the Phase II CORE Seal will be promoted in CORE marketing materials and on the CAQH Website.

Phase II CORE® Seal Application
version 2.1.0 March 2011

E. Fees

Please review the fee structure and notes below to determine your CORE Seal fee.
Then check the appropriate box under the stakeholder type for the Seal you are requesting.

Health Plans

□ Below $75 million in net annual revenue	$4,000 fee
□ $75 million and above in net annual revenue	$6,000 fee

Clearinghouses

□ Below $75 million in net annual revenue	$4,000 fee
□ *EHNAC HNAP-EHN accredited*	*- apply 10% ($400) discount*
□ $75 million and above in net annual revenue	$6,000 fee
□ *EHNAC HNAP-EHN accredited*	*- apply 10% ($600) discount*

Vendors

□ Below $75 million in net annual revenue	$4,000 fee
□ $75 million and above in net annual revenue	$6,000 fee

Providers

□ Up to $1 billion in net annual revenue	$500 fee
□ $1 billion and above in net annual revenue	$1,500 fee

□ **Endorser**	
(Only for entities that do not create, transmit or use eligibility data.)	No fee

Fee Notes:

1. There is no charge to Federal or State government entities to receive the CORE Seal.
2. There is no charge to CAQH member plans to receive the CORE Seal.
3. This fee is a one-time cost for Phase I certification, unless an entity becomes decertified or if substantive changes to the rules are approved by a full CORE vote (Reference Phase II CORE 202 Certification Policy, version 2.1.0.)
4. Per the Phase I CORE 102 Eligibility and Benefits Certification Policy, vendor products, and not entire vendor organizations, receive the Certification Seal.
5. The CORE Certification Seal fee does not include the fee for CORE certification testing. See http://www.caqh.org for a list of CORE-authorized testing companies and their associated testing fees.
6. Any Clearinghouse/EHN entity actively seeking CORE certification as of June 1, 2009 or later that has already achieved EHNAC HNAP-EHN accreditation can take advantage of the partnership program discount. The Clearinghouse/EHN will indicate that it holds a current EHNAC HNAP-EHN accreditation when submitting a CORE Seal application. (CAQH will confirm EHNAC-EHN accreditation status independently.)

After reviewing this document and ensuring you have all the required documentation, please submit your check and required certification and testing documentation to:

CAQH
RE: Phase I CORE Seal
601 Pennsylvania Ave, NW
South Building, Suite 500
Washington, DC 20004
Email: CORE@caqh.org Fax: 202-861-1454

Phase II CORE® HIPAA Attestation Form*

version 2.1.0 March 2011

[_____] ("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 X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 and ASC X12 005010X212 Health Care Claim Status and Response (276/277) Technical Report Type 3 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

Please submit this form along with your organization's Phase II CORE Seal Application.

**For Entities Seeking Phase II CORE Certification. If your organization is seeking CORE-Endorsement, please refer to the CORE Endorsement Overview*

GUIDING PRINCIPLES

- *After signing the CORE Pledge and/or Addendum, 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 II CORE Operating 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 Phase II CORE certification testing, CORE entities will receive a Phase II CORE certification "CORE Seal" from CAQH.*
- *Entities seeking Phase II CORE certification will be required to adopt all of Phase II CORE Operating Rules that apply to their business and will be responsible for all their own company-related testing costs.*
- *Entities undergoing Phase II CORE certification testing must be Phase I CORE certified or concurrently testing for compliance with Phase I Operating Rules, except in the case of vendors and clearinghouses that do not conduct eligibility v5010 270/271 transactions. (e.g., vendors/clearinghouses that offer only v5010 276/277 claim status transactions can become Phase II certified without being Phase I certified.)*
- *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 v5010 270/271 and/or v5010 276/277 transaction(s). 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 compliant v5010 270/271 and v5010 276/277 transactions.*
- *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 and/or claim status information)*
  - *A parent corporation seeking certification will not be certified unless all subsidiaries of the corporation are with compliant CORE Operating 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.*
- *If a CORE-certified entity begins offering a new transaction for which CORE certification exists, or it acquires an organization that offers the transaction, the entity will have 12 months to certify that new transaction; if the CORE-certified entity does not certify for the new transaction, it will lose its CORE Seal.* (*Note: An entity has 180 days to complete CORE Certification Testing once the Pledge has been signed.*)
- *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 Phase II CORE certification will be charged two fees: fees related to CORE certification testing as determined by the CORE-authorized Testing Vendor 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 Operating Rules throughout any system upgrades. When vendors release new versions of their products that affect the functionality of CORE Operating 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 Operating Rules is established by vote. Revisions will not be made to the CORE Operating Rules more than once (1) per year. Revisions to approved CORE Operating Rules, if necessary, will become official 20 business days after enacted by CORE. (Version is defined as a substantive change to any approved Phase of CORE Operating Rules that requires full CORE membership consent.) Although revisions to the rules will become official 20 business days after enacted by CORE, CORE-certified entities will determine when/if they will become in conformance with new phases of the rules.

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 Vendors if they meet certain criteria.

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

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

- Certification testing will differ by role of generator/submitter in the eligibility and/or claim status request transaction.
- Any fee/cost imposed by a CORE-authorized Testing Vendor 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 Vendor; thus prices will be market-driven.

- If a vendor or clearinghouse does not offer a product/service for which CORE certification exists in Phase II, it must submit an attestation to this fact.
- A CORE-authorized Testing Vendor 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 Vendor demonstrating the entity's compliance with CORE Operating Rules through successful testing.

- CORE will be responsible for providing the official CORE 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 v5010 270/271 and/or v5010 276/277 claim status transactions (or, in the case of a vendor, supports the v5010 270/271 and/or v5010 276/277 claim status transactions).
  - 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. CORE will report on its website:
  - List of certified entities.
  - In the case of vendors and clearinghouses, the CORE-certified transaction(s) processed by their product.
- The fee for the Phase II CORE Seal will be the same as the Phase I CORE Seal fee, regardless of the number of transactions for which an entity has completed Phase II testing.
- The cost of the CORE Seal will be a one-time fee, unlike the CORE participation fee, which is an annual fee. The CORE Seal indicates that an entity/product is CORE-certified, while the CORE participation fee allows entities to participate in the CORE Operating 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 Operating 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, recertification 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 CORE Seal is valid and current.

Subsection 3.4: (Potential) Step 4: Recertification will be required if an entity's CORE 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: Recertification 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 recertification (see CORE version control document).
- Major substantive changes, e.g., new phases, will require recertification 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, recertification will be required only after CORE membership approves, by vote, major modifications, changes, or deletions to CORE Operating Rules.
- Generally, CORE Operating Rules will not be amended between CORE Operating Rule phases unless government regulations are issued that impact the CORE Operating 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 to 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 Vendor to re-test the results in question within 21 business days of request.
- The CORE Enforcement Committee will have oversight of this process. Please see the Phase II CORE 205 Enforcement Policy version 2.1.0 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 X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 and ASC X12 005010X212 Health Care Claim Status and Response (276/277) Technical Report Type 3 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

Phase II CORE 203 Certification Exemption Policy
version 2.1.0 March 2011

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 Phase II CORE 202 Certification Policy version 2.1.0.

- *Entities may seek certification for their subsidiaries versus their corporate entity. The CORE 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 decertified (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 CORE compliant 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 t*o the exemption policy.
- If a certified heath 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 decertified, the health plan will need to reapply for CORE certification.
- The Phase II CORE 205 Enforcement Policy outlines the steps to become recertified after being decertified. Health plans wanting to become recertified due to non-compliance with an IT exemption rule will need to be recertified for all transactions for which CORE certification exists.

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

- All CORE-certified entities will be listed on the CAQH website (see Phase II CORE 202 Certification Policy version 2.1.0). In addition, Phase II certified vendors and clearinghouses will have the transaction(s) listed for which they have certified.
- 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.

Phase II CORE® Certification
Health Plan IT Exemption Request Form
version 2.1.0 March 2011

A. Contact Information

Organization: _____

Contact Name: _____

Mailing Address: _____

Phone: _____

Email: _____

B. 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:

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.

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).

C. 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.

D. Required Documents

Please attach the following with this application:

1. HIPAA Attestation Form (signed by your organization's appropriate senior executive).

2. A list of the states, markets and systems for which the exemption applies. The list should provide enough detailed information for providers to easily determine when your health plan will begin providing CORE compliant transactions in their practice area.

By signing this form, your organization is stating that your health plan meets the agreed-upon IT system exemption criteria.

Signature: _____

Name: _____

Title: _____

Please submit this form with your CORE Seal Application.

 Please contact CAQH at CORE@caqh.org or (202) 861-6380 with questions.

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 Testing Vendors through a standard CORE evaluation process will be used by interested parties to test for CORE Operating Rules compliance. CORE will authorize any testing vendor that meets CORE's testing vendor criteria. A key criteria in becoming a CORE-authorized Testing Vendor will be that the entity is capable of testing for all Phase I and Phase II Operating Rules.*
- *A prerequisite for obtaining a stakeholder-specific CORE Seal will be the successful completion of a stakeholder-specific Phase II CORE Certification Test Suite, which will be demonstrated through proper documentation from a CORE-authorized Testing Vendor.*
- *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 Operating 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 precertification, 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 testing process

- A CORE-authorized Testing Vendor performs testing with an entity seeking CORE certification based upon Phase II CORE testing criteria specific to the participant's stakeholder type.
- Entities seeking CORE certification can work with the CORE-authorized Testing Vendor of their choice to test and/or use a testing website developed by one or more of the companies to conduct their Phase II CORE certification testing. If website approach is taken, individual company testing results would not be shared publicly. The Phase II CORE Certification Test Suite includes scenario-based testing and expected outcomes.
- The Phase II CORE Certification Test Suite focuses on current industry eligibility and claim status 'pain points' and therefore includes testing that builds on the Phase I CORE Operating Rules as well as new Phase II Operating Rules for claim status requests and improved patient identification, including the following:

Phase II CORE Operating Rule	Key Aspect of CORE Stakeholder-Specific Testing[1,2]			
	Providers	Health Plans	Vendors	Clearinghouses
ELIGIBILITY				
Connectivity Rule[4]	Yes	Yes	Yes[3]	Yes[3]
V5010 270/271 Data Content Rule[4]	Yes	Yes	Yes[3]	Yes[3]
Last Name Normalization Rule	Yes	Yes	Yes[3]	Yes[3]
Use of AAA Error Codes Rule	Yes	Yes	Yes[3]	Yes[3]
CLAIM STATUS				
Acknowledgements Rule: Batch and Real Time	Yes	Yes	Yes[3]	Yes[3]
Companion Guide	Yes	Yes	Yes[3]	Yes[3]
Connectivity	Yes	Yes	Yes[3]	Yes[3]
Response Time: Batch and Real Time	Yes	Yes	Yes[3]	Yes[3]
System Availability	No	Yes	Yes[3]	Yes[3]

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 Phase II CORE Seal by sending documentation to CORE. (Certification Process begins, please see Phase II CORE 202 Certification Policy version 2.1.0.)

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 to 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 Phase II 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 CORE Enforcement Committee (please see Phase II CORE 205 Enforcement Policy version 2.1.0.)
- CORE will have 20 business days to investigate the issue. If the appeal is deemed valid, CORE will ask the CORE-authorized Testing Vendor to re-test the results in question within 21 business days of request.

[1] 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.
[2] As in Phase I, certification in Phase II is not exhaustive.
[3] Compliance is only required for the transaction(s) offered by the entity. If a Vendor or clearinghouse does not offer a product/service for which CORE certification exists in Phase II, it must submit an attestation to this fact.
[4] Phase II CORE Operating Rule builds upon the Phase I CORE Operating Rule

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 Operating 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 CORE Enforcement Committee.*
- *The CORE 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 Noncompliance, 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 CORE 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 Operating 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 retesting for compliance with the rule(s) or be decertified.

- 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 noncompliance. If a member of the CORE 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 CORE 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 CORE 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 CORE 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: Decertification/removal of CORE Seal.

Section 4: For Decertified Entities Interested in Recertification

Subsection 4.1: Step 1: A decertified entity may seek recertification; entities are responsible for all fees associated with recertification, including any fees for a new CORE Seal.

- Entities seeking recertification 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 Vendors will provide documentation on the entity's compliance with the rule specific to the applicable CORE Certification 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 to 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 Operating 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

CORE: Non-Compliance Complaint Form			
Please provide your contact information (All fields required.)			
Organization Name and Type (Health Plan, Provider, Clearinghouse, Vendor)			
Name (First and Last)			
Street Address	**City/Town**	**State**	**Zip**
Telephone Number		**Email Address**	
Organization filing complaint against (All fields required.)			
Organization Name and Type (Health Plan, Provider, Clearinghouse, Vendor)			
Name (First and Last)			
Street Address	**City/Town**	**State**	**Zip**
Telephone Number		**Email Address**	
When did this alleged violation occur? mm/dd/yyyy (Required field) **1.** **2.** **3.** **4.** **5.**			
Have efforts been made to address the problem? Who at the company in question have you been			

CORE: Non-Compliance Complaint Form
working with to resolve the issue?
Identify the CORE Operating Rules complaint category. (Required field.) Select one category listed below per complaint submission. Complete this form again to file a complaint for another category.
Eligibility □ Response Time □ System Availability □ Service Type and Benefit Summary □ Patient Financial Responsibility □ Acknowledgements □ Connectivity □ Companion Guide □ Last Name Normalization □ Use of AAA Error Codes **Claim Status** □ Acknowledgements □ Companion Guide □ Connectivity □ Response Time □ System availability
Describe, in detail, the alleged violation. (Required field.) You may attach/upload additional pages as needed. Please enclose at least five examples of your complaint.
Please sign and date this complaint. (Required field) **SIGNATURE:** **DATE:**

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 Operating 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 Phase II CORE 205 Enforcement Policy version 2.1.0 Section 2.

Table of Contents

1 BACKGROUND SUMMARY

Phase I CORE Rules focus on improving electronic eligibility and benefits verification, as eligibility is the first transaction in the claims process. Thus, if eligibility and benefits are correct, all the transactions that follow will be more effective and efficient. Building on this, CORE determined that the Phase II CORE rules should be extended to include rules around the claim status transaction that allow providers to check the status of a claim electronically, without manual intervention, or confirm claims receipt. Benefits to electronic claim status inquiry and response will provide for:

- Less staff time spent on phone calls and websites
- Increased ability to conduct targeted follow-up
- More accurate and efficient processing and payment of claims

The inclusion of this Phase II CORE rule for the HIPAA-adopted ASC X12 005010X212 Health Care Claim Status Request and Response (276/277) Technical Report Type 3 (TR3) implementation guide and associated errata (hereafter v5010 276, v5010 277 or v5010 276/v5010 277) will facilitate the industry's momentum to increase access to the claim status transaction, and will encourage CORE-certified entities to use the infrastructure they have for the HIPAA-adopted ASC X12 005010X279A1 Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 implementation guide and associated errata (hereafter v5010 270/271), and apply this infrastructure to claims status.

2 ISSUE TO BE ADDRESSED AND BUSINESS REQUIREMENT JUSTIFICATION

In order to electronically process a claim status inquiry, providers need to have a robust v5010 277 claim status response. This robust response includes the health plans providing the status of the claim, such as pre-adjudication acceptance or rejection, an incorrect or incomplete claim is pended, or that the claim is suspended and additional information is being requested. HIPAA provides a foundation for the electronic exchange of claim status information, but does not go far enough to ensure that today's paper-based system can be replaced by an electronic, interoperable system. HIPAA's mandated data scope does not require the financial information needed by providers, and HIPAA neither addresses the standardization of data definitions nor contains business requirements by which the HIPAA-outlined data can flow efficiently and on a timely basis.

Using the available but not-required (situational) elements of the v5010 276/v5010 277, the Phase II CORE 250: Claim Status Rule defines the specific business information requirements that health plans must satisfy and which vendors, clearinghouses and providers should use if they want to be CORE-certified. As with all CORE rules, these requirements are intended as a base or minimum set of requirements and it is expected many CORE-certified entities will add to these requirements as they work towards the goal of administrative interoperability. The Phase II CORE 250: Claim Status Rule requires that health plans respond to an inquiry in real time (within 20 seconds), make appropriate use of the standard acknowledgements to eliminate the "black hole," support the CORE "safe harbor" connectivity requirement, and ensure that the system components required to process claim status inquiries are available 86% of the time.

By requiring the delivery and use of this claim status information via the v5010 276/v5010 277, the Phase II CORE 250: Claim Status Rule helps provide the information that is necessary to electronically process a claim status inquiry and thus reduce the current cost of today's paper-based transaction process.

3 SCOPE

3.1 What the Rule Applies To

The Phase II CORE 250 Claim Status Rule builds upon and extends the Phase I CORE Infrastructure rules to the conduct of the v5010 276/v5010 277. This rule specifies that a CORE-certified entity must conduct these transactions in real time, respond within 20 seconds, make their systems available 86 % of the time, use the ASC X12 standard acknowledgments and support the CORE connectivity safe harbor requirements.

3.2 When the Rule Applies

This rule applies when a Phase II CORE-certified entity uses, conducts, or processes the v5010 276/v5010 277 claims status transactions.

3.3 What the Rule Does Not Require

This rule does not address any v5010 276/v5010 277 transaction content requirements of the v5010 276/v5010 277 implementation guide. All Phase II rules applicable to claims status are related to improving access to the transaction, *not* addressing content requirements. This decision was made due to:

- The considerable amount of content requirements in other Phase II rules applicable to the v5010 270/271 eligibility transactions.
- The need for standard setting bodies to address content issues with claims status, e.g., agreement on status codes.

This rule does not require any entity to:

- Conduct, use, or process the v5010 276/v5010 277 claim status transactions if it currently does not do so.
- Integrate its current claim status processing system components into its current eligibility processing system if they are not currently integrated.

3.4 Outside the Scope of This Rule

This rule does not address the data content of the v5010 276 nor the data content of the health plan's response using the v5010 277.

3.5 How the Rule Relates to Phase I CORE

This rule applies the Phase I CORE infrastructure rules (e.g., Response Time, System Availability, Acknowledgements, and Companion Guide), which were created to increase access to the v5010 270/271 transactions, and applies these rules, where appropriate, to the v5010 276/v5010 277 claim status transactions.

As with other Phase II rules, general CORE policies also apply to Phase II rules and will be outlined in the Phase II CORE rule set. The CORE policies include:

- Certification testing for each stakeholder wishing to be awarded a CORE-certified Seal
- Entities seeking CORE-certification may use a contracted party to meet CORE rules, e.g. some providers meet CORE connectivity requirements via their vendor products
- A health plan system exemption policy for system migration
- Entities only need to test for and meet batch rule requirements if they currently offer batch for claim status transactions. A CORE guiding principle is to move to real time; thus, CORE rules do not require entities to build batch capabilities.

3.6 Assumptions

The following assumptions apply to this rule:

- This rule is a component of the larger set of Phase II CORE rules; as such, all the CORE Guiding Principles apply to this rule and all other rules.
- All entities seeking Phase II certification must be Phase I CORE-certified as the Phase I CORE rules provide a foundation for the Phase II CORE rules. The exception is vendors/clearinghouses that do not conduct v5010 270/271 eligibility transactions.
- This rule is not a comprehensive companion document addressing any content requirements of either the v5010 276 Claim Status Request or v5010 277 Claim Status Response transaction sets.
- Compliance with all CORE rules is a minimum requirement; a CORE-certified entity is free to offer more than what is required in the rule.
- Providers, vendors, clearinghouses and health plans (or other information sources) all need to meet appropriate aspects of the rule and all will be tested via CORE certification testing.

4 RULE

4.1 Claim Status Connectivity Requirements

These requirements address proposed usage patterns for both batch and real time transactions, the exchange of security identifiers, and communication-level errors and acknowledgements. It does not attempt to define the specific content of the message exchanges beyond declaring that the HIPAA-adopted ASC X12 formats must be used between covered entities and security information must be sent outside of the ASC X12 payloads.

These requirements are 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 the Phase II CORE 270: Connectivity Rule version 2.2.0 to support v5010 of the ASC X12 administrative transactions, whether or not adopted by HIPAA. These requirements are 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 these requirements.

These requirements describe some of the specifics for implementing HTTP/S connectivity for healthcare administrative transaction exchange.

4.2 Claim Status Real Time Acknowledgement Requirements

These requirements assume a successful communication connection has been established and that all parties in the transaction routing path are CORE-certified.

These requirements address only acknowledgements for receivers of the v5010 276 for Real Time. It does not address acknowledgements that receivers of the v5010 277 must consider.

4.2.1 Use of the v5010 999 and v5010 277 Acknowledgements for Real Time

4.2.1.1 Reporting on a Real Time v5010 276 Submission That Is Rejected

Functional Group or Transaction Set Rejection

If the v5010 276 passes ASC X12 Interchange editing, but an 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 v5010 276 (clearinghouse, intermediary, health plan or information source) must always return an

ASC X12 005010X231A1 Implementation Acknowledgement for Health Care Insurance (999) (hereafter v5010 999) for the Functional Group of the v5010 276 inquiry to indicate a rejection (negative acknowledgement). If the Functional Group is not rejected, a v5010 999 must not be returned.

4.2.1.2 Reporting on a Real Time v5010 276 Submission that is Accepted

If the v5010 276 complies with the ASC X12 v5010 276 TR3 implementation guide requirements, then the v5010 277 Claim Status Response will be returned to the submitter.

Therefore the submitter of a v5010 276 in real time will receive only one acknowledgement/response from the receiver (clearinghouse, intermediary, health plan or information source): a v5010 999 (rejection); or a v5010 277.

4.2.2 Conformance

Conformance with this section's requirements are considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach is similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

Per the Phase II CORE Certification Test Suite, conformance with this rule is considered achieved by receivers of the v5010 276 (clearinghouse, intermediary, health plan or information source) if all of the following criteria are achieved:

1. A v5010 999 is returned only to indicate a Functional Group (including the enclosed Transaction Set) error resulting in the rejection of the entire Functional Group.
    a. A v5010 999 must not be returned if there are errors not resulting in the rejection of the Functional Group and enclosed Transaction Set.
2. A v5010 277 must always be returned for an Interchange, Functional Group and Transaction Set that complies with ASC X12 v5010 276 requirements.
    a. A v5010 277 may contain either the appropriate STC Claim or Line Level Status Information segment(s) in the case of a business level error or the data segments containing the requested claim status details.

4.3 Claim Status Batch Acknowledgement Requirements

These requirements for use of acknowledgements for batch mode places parallel responsibilities on both submitters of the v5010 276 (providers) and submitters of the v5010 277 (health plans or information sources) for sending and accepting the v5010 999. *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.

4.3.1 Use of the v5010 999 Acknowledgement for Batch v5010 276 and v5010 277

The receiver of the batch (the provider, clearinghouse, intermediary, health plan or information source) must always return a v5010 999 for each Functional Group of a v5010 276 batch or a v5010 277 batch to indicate that the Functional Group was either accepted, accepted with errors, or rejected.

4.3.2 Requirements for Return of a v5010 999

The v5010 999 must not be returned during the initial communications session in which the v5010 276 batch is submitted. *See §4.5 Claim Status Batch Response Time Requirements for the timing and availability of ~~t~~his acknowledgement.*

4.3.3 Conformance

Conformance with this section's requirements is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach is similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the CORE Phase II Certification Test Suite for details.

Per the Phase II CORE Certification Test Suite, 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 v5010 999 is returned to indicate acceptance, rejection or errors in a Functional Group (including the enclosed Transaction Set).
    a) A v5010 999 must always be returned even if there are no errors in the Functional Group and enclosed Transaction Set.
2. A v5010 277 response transaction must always be returned for an Interchange, Functional Group and Transaction Set that complies with ASC X12 TR3 implementation guide requirements.

4.4 Claim Status Real Time Response Time Requirements

Maximum response time when processing in real time mode[1] for the receipt of a v5010 277 (or in the case of a rejection, a v5010 999) from the time of submission of a v5010 276 must be 20 seconds (or less). V5010 999 response rejections must be returned within the same response timeframe.[2] *See §4.6 Claim Status System Availability Requirements for notification process of holidays.*

4.4.1 Conformance Measurement

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.

4.4.2 Conformance

Conformance with this section's requirements is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach is similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires

[1] Real time mode is defined in the CORE Glossary of Terms.
[2] See §4.2 Claim Status Real Time Acknowledgement Requirements, which requires return of either a v5010 999 or a v5010 277 response.

entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

The Phase II CORE Certification 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.

4.5 Claim Status Batch Response Time Requirements

When a v5010 276 batch submitted in batch processing mode is 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 v5010 277, the Claim Status Batch Response Time Requirements shall apply. *(See §4.4 Claim Status Real Time Response Time Requirements)*

Maximum response time when processing in batch mode[3] for the receipt of a v5010 277 batch to a v5010 276 batch submitted by a provider or on a provider's behalf by a clearinghouse/switch by 9:00 pm Eastern time of a business day must be returned by 7:00 am Eastern time the following business day. A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (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 §4.6 Claim Status System Availability Requirements for notification process of holidays.)*

4.5.1 Batch Response Time v5010 999 Acknowledgement Requirements

A v5010 999 must be available to the submitter within one hour of receipt of the batch: to the provider in the case of a batch v5010 276 and to the health plan (or information source) in the case of a batch v5010 277.[4]

4.5.2 Conformance Measurement

Conformance with this maximum response time requirement 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 requirement 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.

4.5.3 Conformance

Conformance with this section's requirements is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed. For Phase II, the certification testing approach is be similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as

[3] Batch mode is defined in the CORE Glossary of Terms

[4] See §4.3 Claim Status Batch Acknowledgements Requirements, which requires return of a v5010 999 in all cases indicating rejection/acceptance of the batch.

testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

The CORE Test Suite for this rule includes the following:

- 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 Phase II CORE 205 Enforcement Policy version 2.1.0 for details on filing complaints and who is permitted to file complaints.
- All CORE-certified entities are required to conform to this rule regardless of the connectivity mode and methods used between CORE-certified trading partners.
- This rule assumes that all parties in the transaction routing path are CORE-certified and compliant.

4.6 Claim Status System Availability

Many healthcare providers have a need to determine the status of a claim that has been submitted for adjudication outside of the typical business day and business hours. Additionally, many institutional providers are now allocating staff resources to performing administrative and financial back-office activities on weekends and evenings. As a result, providers have a business need to be able to conduct claim status transactions at any time.

On the other hand, health plans have a business need to take their claims processing and other systems offline periodically in order to perform the required system maintenance. This typically results in some systems not being available for timely v5010 276 and v5010 277 certain nights and weekends. The rule was created to address these conflicting needs.

4.6.1 System Availability Requirements

System availability[5] must be no less than 86 percent per calendar week[6] 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.

4.6.2 Reporting Requirements

4.6.2.1 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.

4.6.2.2 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.

4.6.2.3 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.

4.6.2.4 No Response Required

No response is required during scheduled downtime(s).

---

[5] System is defined as all necessary components required to process a v5010 276 and v5010 277.
[6] Calendar week is defined as 12:01 am Sunday to 12:00 am the following Sunday.

4.6.2.5 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.

4.6.3 Conformance

Conformance with this rule is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach is similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

Per the Test Suite, each CORE-certified entity must demonstrate its conformance with this system availability rule by publishing the following documentation:

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

4.7 Claim Status Companion Guide

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 ASC X12 v5010 TR3 implementation guide, 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 ASC X12 v5010 Implementation Guide. To address this issue, CORE developed the CORE v5010 Master 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 v5010 Master Companion Guide Template gives health plans the flexibility to tailor the document to meet their particular needs.

Note: The CORE v5010 Master Companion Guide Template has been adapted from the CAQH/WEDI Best Practices Companion Guide Template originally published January 1, 2003.

4.7.1 Claim Status Companion Guide Requirements

All CORE-certified entities' Companion Guides covering the v5010 276/v5010 277 transactions must follow the format/flow as defined in the CORE v5010 Master Companion Guide Template.

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.

4.7.2 Conformance

Conformance with this section's requirements is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach is similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

Per the Test Suite, 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 v5010 276 and the v5010 277 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 v5010 276/v5010 277 companion guide.
    b) A copy of a page of its official v5010 276/v5010 277 companion guide depicting its conformance with the format for specifying the v5010 276/v5010 277 data content requirements.
    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 v5010 276/v5010 277 content requirements of the companion guide is located.

Acme Health Plan

HIPAA Transaction
Standard Companion Guide

Refers to the Implementation Guides
Based on ASC X12 version 005010

CORE v5010 Master Companion Guide
Template

March 2011

Disclosure Statement

This document …

Preface

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

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

This section describes how ASC 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 ASC 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).

Table of Contents

1 BACKGROUND

The unique identification of an individual is not only an essential requirement for the successful use of the HIPAA-adopted ASC X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 Implementation Guide (hereafter v5010 270/271, v5010 270, v5010 271), but is also a critical component of identity management – which includes authentication, authorization, transaction control, audit, etc. As the U.S. healthcare community continues to accelerate the move to electronic health records (EHR) and personal health records (PHR) it is increasingly important that the exchange of individual names and other demographic data between healthcare providers and health plans be standardized to the extent reasonable and practicable.

The development of a comprehensive standard for the unique identification of individuals in healthcare is not within the scope of CORE. However, it is reasonable for CORE to develop various rules addressing certain aspects of the identification of individuals that will enhance the automated real time processing of eligibility inquiries and responses. Such CORE rules can, and should be, wherever possible, based on the work of existing standards development organizations.

One such standard being developed is the "Identification of Subjects of Health Care" by the ISO Technical Committee 215 – Health Informatics. ANSI serves as the secretariat for TC 215, and key members from the U.S. include HL7, HIMSS/IHE, ASTM, and the American Dental Association. This standard under development includes detailed specifications for the use of titles, name suffixes, special characters and punctuation in text fields for an individual's first name, middle name, last name, among others. Since the ASC X12 standards do not address the use of name suffixes, special characters and punctuation in text data elements for names of organizations and individuals, this CORE rule draws heavily on the TC 215 standard currently under development.

2 ISSUE TO BE ADDRESSED AND BUSINESS REQUIREMENT JUSTIFICATION

Healthcare providers and health plans have a requirement to uniquely identify patients (aka subscribers, members, beneficiaries) for the purpose of ascertaining the eligibility of the patient for health plan benefits. At a high level, this identification requirement consists of accurately matching:

- Individuals with records and information that relate to them and to no one else; and
- Disparate records and information held in various organizations' computer systems about the same individuals.

For health plans, this identification requirement currently is met by uniquely numbering the individuals whereby each person (or a subscriber and dependents) is assigned an identifier by the health plan covering the individual, i.e., a subscriber, member or beneficiary ID. This ID is combined with other demographic data about the individual (e.g., first name, last name, date of birth, gender, etc.) and then used in healthcare transactions, such as eligibility inquiries, claims submissions, etc. Healthcare providers obtain this unique identifier from patients, combine it with other demographic data, and then subsequently use it when conducting electronic transactions with health plans, such as insurance verification and claims submissions. The health plans then use this combination of ID and demographic data to attempt to uniquely locate the individual within their systems. However, oftentimes, while the ID may be valid and correct, the other demographic data submitted by the healthcare provider does not match similar demographic data held by the health plans' systems, and such transactions are then rejected or denied.

2.1 Issues with Special Characters

The results from the CORE Patient ID Survey indicate that two-thirds of health plan respondents use special characters as submitted in the matching process and require an exact match on them. The remaining one-third of health plan respondents report that some remove special characters and spaces, convert certain characters to spaces, or do not allow special characters to be used in the name data elements. Thus, the impact to healthcare providers submitting names with special characters embedded can result in a significant percentage of query rejections if the data as submitted does not match exactly with what the health plan has in its system.

How Are Special Characters Handled in a Search?	Number of Respondents
Used in search and require an exact match	10
Remove special characters and spaces	2
Convert certain characters to spaces	1
Not allowed	1
Combination of approaches	1
Total	15

The use of upper case characters in name data elements appears not to present as significant an impact to potential query rejections since all but two health plans reported they either ignore character case or convert lower case characters to all caps prior to performing a search.

How Are Upper/Lower Case Characters Handled in a Search?	Number of Respondents
Used in search and require an exact match	2
Case is ignored or converted to all caps	11
Total	13

Even though the HIPAA-adopted v5010 270/271 Implementation Guide specifies the data elements and data element attributes (e.g., data type, min/max number of characters, etc.) that may be used to identify an individual, the underlying ASC X12 standards do not address one critical aspect of demographic data: requirements and/or restrictions on the use of punctuation and special characters. On the other hand, the ASC X12.6 Application Control Structure v005010 (hereafter X12.6) standard requires the use of the Basic Character Set (which allows only uppercase letters) unless the two trading partners agree to use the Extended Character Set (which includes lowercase letters). See X12.6 § 3.3.1 and § 3.3.2 for the complete specification of character sets.

2.2 Issues with Last Name Suffixes and Prefixes

The results from the CORE Identifiers Subgroup preliminary research indicate that it is very difficult to standardize suffix and prefix data entry requirements. Additional challenges identified include:

- No guidance on definition of legal name or allowable suffixes and prefixes
- Different types of suffixes in use:
  - Academic (Ph.D., M.D.)
  - Honorary/professional (Esq., CPA, FHFMA, etc.)
  - Birth Order or Social (Jr., Sr., III)
- Prefixes include forms of address, e.g., Mr., Ms., Dr., Rev., etc.
- Unknown volume of names with suffixes and prefixes in health plan/provider databases (initial CORE survey did not include this although one health plan estimated that 4% of names in its database contain a suffix)

The impact on healthcare providers submitting names with name suffixes or prefixes either separately or embedded with the last name can result in a reasonable percentage of query rejections if the data as submitted do not match exactly with what the health plan has in its system. CAQH survey responses of CORE Identifiers Subgroup participants regarding issues for name suffixes showed the following variations in suffix handling:

- Some systems have capability to store suffix as separate data element
- Some systems with capability to store suffix separately do not enforce this during data entry
- Some systems have entered the suffix as part of the last name field in order to meet Medicare's previous exact match requirements
- Some systems have a single field for full name with each name component delimited by a comma
- Some systems have a single field for full name with each name component delimited by either a comma or a space and no delimiter for suffix
- Some systems with delimited name fields parse name into separate components in the v5010 270

Table of Last Name and Suffix Examples

NM103: Last Name	NM107: Suffix
Smith-Wesson Sr.	
Smith-Wesson, Sr.	Sr.
Smith-Wesson Sr., M.D.	
Smith-Wesson, M.D. Sr.	
SMITH SR	
SMITHSR	
SMITH	SR
Smith-Wesson, Jr., MD, FHFMA	
Smith-Wesson, Esq.	

Although not separately surveyed, CORE participants' analyses indicate that the issue with prefixes being embedded into the NM103 Last Name field is no different from the suffix issue.

3 SCOPE

3.1 What the Rule Applies To

This CORE Rule applies to the HIPAA-adopted v5010 270/271 transactions and specifies the requirements for a CORE-certified health plan (or information source) to normalize a person's last name during any name validation or matching process by the health plan (or information source).

This CORE rule applies only to certain characters in a person's last name including:

- Punctuation values as specified in §4.2.3
- Upper case letters
- Special characters as specified in §4.2.3
- Name suffixes and prefixes specified as character strings in §4.2.2

3.2 When the Rule Applies

This CORE rule applies only when:

- The trading partners are using the ASC X12 Basic Character Set (see §3.6. below for explanation).

And

- A member ID (MID) is submitted in Loop 2100C of the v5010 270 inquiry transaction

And

- A Last Name (LN) is submitted in Loops 2100C/2100D of the v5010 270 inquiry transaction

And

- The Last Name (LN) is used in the health plan's (or information source's) search and match logic.

3.3 When the Rule Does Not Apply

This CORE rule does not apply when:

- Trading partners have agreed to use the ASC X12 Extended Character Set

Or

- The Last Name (LN) is not used in the health plan's (or information source's) search and match logic.

3.4 Recommendation for Validation of Last Name in Other Transactions

Health plans are encouraged to employ a no-more-restrictive name validation logic in other HIPAA administrative transactions than what is employed for the v5010 270/271 transactions.

3.5 Applicable Data Elements & Loops

This rule covers the following specified data element and loops in the v5010 270 and v5010 271 transactions:

Loop ID and Name
Loop 2100C Subscriber Name
Data Element Segment Position, Number & Name
NM103-1035 Last Name
AAA03-901 Reject Reason Code
INS03-875 Maintenance Type Code
INS04-1203 Maintenance Reason Code
Loop ID and Name
Loop 2100D Dependent Name
Data Element Segment Position, Number & Name
NM103-1035 Last Name
AAA03-901 Reject Reason Code
INS03-875 Maintenance Type Code
INS04-1203 Maintenance Reason Code

3.6 Outside the Scope of this Rule

This rule does not:

- Require CORE-certified entities to internally store these and other data elements in conformance with this rule, but rather requires that all parties conform to this rule when conducting the HIPAA-adopted v5010 270/271 transactions electronically;
- Require conversion of letter case and/or special characters by any party for subsequent processing of the data through internal systems;
- Specify whether or not a health plan (or information source) must validate the full last name or may validate only a portion of the last name;
- Specify the search criteria used by a health plan (or information source) to identify a patient;

3.7 Approved Basic Character Set

The ASC X12 Basic Character Set consists of:

(1) Upper case letters from A to Z

(2) Digits from 0 to 9

(3) Special characters

! " & ' ( ) * + , - . / : ; ? =

(4) The space character

Note: Special characters are removed from this category when used as delimiters.

3.8 Use of Extended Character Set

The ASC X12 Extended Character Set as specified in X12.6 Application Control Architecture §3.3.2 is outside the scope of this rule and may be used only by agreement between trading partners. The ASC X12 Extended Character set includes the lowercase letters, other special characters, national characters and select language characters.

3.9 Assumptions

The following assumptions apply to this rule:

- This rule is a component of the larger set of Phase II CORE rules; as such, all the CORE Guiding Principles apply to this rule and all other rules;
- All entities seeking Phase II CORE certification must first be Phase I CORE-certified as Phase I CORE provides a foundation for Phase II CORE;
- Requirements for the use of the applicable loops and data elements apply only to the HIPAA-adopted v5010 270/271;
- Health plans (and information sources) are able, in a reasonable timeframe, to maintain the relevancy, accuracy, and timeliness of data returned in the v5010 271;
- This rule is not a comprehensive companion document specifying the complete content of either the v5010 270 or v5010 271 transactions. The focus in this rule is on specifying requirements for the v5010 271 to address the Phase II CORE Last Name Normalization requirements;
- The submitter of the v5010 270 knows which data elements and values were submitted in the v5010 270 (i.e., member identifier, first name, last name, date of birth).

4 RULE

4.1 Basic Recommendations for Submitters of the v5010 270

4.1.1 When Name Suffix is Stored Separately

When the submitter's system enables the capture and storage of a person's name suffix in a separate data field, the person's name suffix should be submitted in the NM107-1039 Name Suffix data element in Loops 2100C/2100D.

4.1.2 When Name Suffix is Not Stored Separately

When the person's name suffix is stored internally as part of a person's last name, the submitter's system must attempt to identify and parse the last name data element to extract the name suffix such that it will be transmitted in the NM107-1039 Name Suffix data element in Loops 2100C/2100D.

When a name suffix or prefix cannot be stored separately, it should be separated from the last name by a space, a comma or a forward slash (see §4.2.3) when storing it.

4.2 Basic Requirements for Health Plans & Information Sources

4.2.1 Normalizing Last Name

A health plan (or information source) must:

normalize the last name as submitted in the v5010 270 inquiry

AND

normalize the last name as stored in the health plan's (or information source's) eligibility system

prior to using the submitted last name and the stored last name.

To normalize the submitted and stored last name:

remove all of the character strings specified in §4.2.2 when they are preceded by one of the punctuation values specified in §4.2.3 and followed by a space or when they are preceded by one of the punctuation values specified in §4.2.3 and are at the end of the data element

AND

remove the special characters specified in §3.7 in the name element.

If the normalized last name is successfully matched or validated, the health plan (or information source) must return the complete v5010 271 as required by the Phase II CORE 260 Eligibility & Benefits (270/271) Data Content Rule (developed as part of Phase II CORE rulemaking).

If the normalized last name is not successfully matched or validated, the health plan (or information source) must return a v5010 271 response with a AAA segment using the appropriate error code as specified in Phase II CORE 259 AAA Error Codes Reporting Rule regarding errors in Subscriber/Patient Identifiers and Names.

4.2.2 Character Strings to be Removed During Name Normalization

The following character strings represent the complete set of character strings to be removed when normalizing a last name as specified in §4.3.1. Any other character strings not included in this section are not covered by this rule. This requirement is in addition to other requirements specified in the Phase II CORE 259: AAA Error Codes Reporting Rule regarding errors in Subscriber/Patient Identifiers & Names.

JR, SR, I, II, III, IV, V, RN, MD, MR, MS, DR, MRS, PHD, REV, ESQ

4.2.3 Punctuation Values Used as Delimiters in Last Name

The following punctuation values represent the recommended set of punctuation values to be used to delimit (separate) a last name from a name suffix or prefix when a name suffix, prefix or a title cannot be stored separately in internal systems.

space, comma, forward slash

4.3 Required Response for Name Validation

If the name validation is successful, the health plan must return the complete v5010 271 as required by the Phase II CORE 260: Eligibility & Benefits (270/271) Data Content Rule (developed as part of Phase II CORE rulemaking).

If the un-normalized stored last name does not match the un-normalized submitted last name, the v5010 271 must include:

the last name as stored prior to normalization in the health plan's (or information source's) eligibility system in the NM103-1035 Last Name data element in either Loop 2100C or Loop 2100D as appropriate

AND

the INS segment with the appropriate codes as specified in Table 4.3 Last Name Validation 271 INS Segment Reporting Requirements below.

Table 4.3 Last Name Validation v5010 271 INS Segment Reporting Requirements

Validation Results	Patient is Subscriber	Patient is Dependent	INS Segment Returned	Code	NM1 Segment Returned
Valid Last Name	Yes	No	2100C	INS03 = 001 Change INS04 = 25 Change in Identifying Data elements	NM103 = Last Name of Subscriber As Stored in Health Plan's Eligibility System
Valid Last Name	No	Yes	2100D	INS03 = 001 Change INS04 = 25 Change in Identifying Data elements	NM103 = Last Name of Patient As Stored in Health Plan's Eligibility System

If the name validation fails, the appropriate AAA error code and other data elements as required by §4.5 of the Phase II CORE 259 AAA Error Codes Reporting Rule regarding errors in Subscriber/Patient Identifiers & Names rule must be returned.

4.4 Basic Requirements for Receivers of the v5010 271

The receiver of a v5010 271 (defined in the context of this CORE rule as the system originating the v5010 270) is required to comply with §4.2 of the Phase II CORE 259 AAA Error Codes Reporting Rule regarding Subscriber/Patient Identifiers & Names.

5 CONFORMANCE REQUIREMENTS

Conformance with this rule is considered achieved when all of the required detailed step-by-step test scripts specified in the CORE Phase II Certification Test Suite are successfully passed.

For Phase II, the certification testing approach will be similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

6 GLOSSARY OF TERMS AND DEFINITIONS USED IN THIS RULE

Term	Definition
Normalize	**1.** To make normal, especially to cause to conform to a standard or norm.[1] **2.** To make (a text or language) regular and consistent, especially with respect to spelling or style.[2] **Text normalization** is a process by which text is transformed in some way to make it consistent in a way which it may not have been before. Text normalization is often performed before a text is processed in some way, such as generating synthesized speech, automated language translation, storage in a database, or comparison. Examples of text normalization: • Unicode normalization • converting all letters to lower or upper case • removing punctuation • removing letters with accent marks and other diacritics • expanding abbreviations While this may be done manually, and usually is in the case of ad hoc and personal documents, many programming languages support mechanisms which enable text normalization.[3]

[1] American Heritage® Dictionary of the English Language, Third Edition
[2] Ibid.
[3] From Wikipedia, the free encyclopedia – http://en.wikipedia.org/wiki/Text_normalization

Table of Contents

1 BACKGROUND

Providers need to have consistent and specific patient identification validation error reporting from health plans in the HIPAA-adopted ASC X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 (TR3) implementation guide (hereafter v5010 270/271, v5010 270, v5010 271) response in order to obtain a robust v5010 271 response so that appropriate follow-up action can be taken to obtain correct information.

§1.4.7.1(7) of the v5010 270/271 TR3 states that: "The information source is also required to return information from any of the following segments supplied in the 270 request that was used to determine the 271 response."

The Phase II CORE Identifiers Subgroup evaluated and considered several approaches for attempting to achieve the goals noted above. Due to the multiple and inconsistent use of AAA error codes by health plans and a variety of search and match approaches used for patient identification, the Subgroup reached consensus on developing a Phase II CORE Rule for specifying a standard and consistent method for reporting AAA errors without specifying the search process utilized by the health plan.

In developing this approach, the Subgroup decided to use the full set of AAA error codes available in v4010A1 271 in order to provide as much specificity as possible within the 271 standard on the reasons for the patient identification error(s). The Subgroup also consulted the v5010 270/271 closely as part of its analysis so that this rule would complement rather than conflict with requirements for error reporting.

2 ISSUE TO BE ADDRESSED AND BUSINESS REQUIREMENT JUSTIFICATION

Healthcare providers and health plans have a requirement to uniquely identify patients (aka subscribers, members, beneficiaries) for the purpose of ascertaining the eligibility of the patient for health plan benefits. At a high level, this identification requirement consists of accurately matching:

- Individuals with records and information that relate to them and to no one else; and
- Disparate records and information held in various organizations' computer systems about the same individuals.

For health plans, this identification requirement currently is met by uniquely delineating the individuals whereby each person (or a subscriber and dependents) is assigned an identifier by the health plan covering the individual, i.e., a subscriber, member or beneficiary ID. This ID is combined with other demographic data about the individual (e.g., first name, last name, date of birth, gender, etc.) and then used in healthcare transactions, such as eligibility inquiries, claims submissions, etc.

Healthcare providers obtain this unique identifier from patients, combine it with other demographic data, and then subsequently use it when conducting electronic transactions with health plans, such as insurance verification and claims submissions. The health plans (or information sources) then use this combination of ID and demographic data to attempt to uniquely locate the individual within their systems. However, oftentimes, the ID may not be valid and correct, the other demographic data submitted by the healthcare provider does not match similar demographic data held by the health plans' systems, or some of the data elements required by the health plan are missing; therefore such transactions are then rejected or denied.

The v5010 270 transaction submitted by healthcare providers may contain some or all of the four data elements in the v5010 270/271 and agreed to in the trading partner agreements. §§1.4.8 and 1.4.8.1 of the v5010 270/271 TR3 define a "maximum data set that an information source may require and identifies further elements the information source may use if they are provided. Section 1.4.8.2 defines four alternate search options that an Information Source is required to support in addition to the Primary Search Option. If an Information Source is unable to identify a unique individual in their system (more than one individual matches the information from the Required Alternate Search Option), the Information Source is required to reject the transaction and identify in the 2100C or 2100D AAA segment the additional information from the Primary Search Option that is needed to identify a unique individual in the Information Source's system."

Among the key findings of the 2006 CORE Patient ID Study (see table below), the following were identified regarding error rates and the disparate use of the AAA error codes:

- Providers and health plan respondents have relatively similar rates of valid 271 responses (78-83%). Clearinghouse respondents have a lower rate of valid 271 responses (70%) but a much higher level of rejections for non-eligibility related reasons, such as system timeout, and system availability issues.
- More generic AAA error codes generally have the highest volume of errors for the v5010 270/271 transactions (e.g., Patient not found, Subscriber/Insured not found).[1]

These findings suggest:

- Improved specificity and standardized use of the AAA codes would give providers better feedback to understand what information is missing or incorrect in order to obtain a valid match.

The following table includes data from the 2006 CORE Patient ID Study about the valid response rate and the utilization of patient-ID related AAA error codes. The table includes data from providers, clearinghouses and health plans. The data show that more specific AAA error codes are rarely used in the current environment.

270/271 ELIGIBILITY INQUIRY RESPONSE - SUMMARY				
Initial Eligibility Inquiry Response DESCRIPTIONS	**AAA Code**	**Providers**	**Health Plans**	**Clearinghouses**
An Inquiry results in a valid response on the 1st pass	**None**	**82.5%**	**77.9%**	**69.5%**
Invalid/Missing Date of Birth	58	0.1%	0.1%	0.3%
Invalid/Missing Patient ID	64	0.4%	0.6%	0.5%
Invalid/Missing Patient Name	65	0.1%	0.1%	0.2%
Invalid/Missing Patient Gender Code	66	0.0%	0.0%	0.0%
Patient Not Found	67	9.2%	1.1%	11.2%
Duplicate Patient ID Number	68	0.0%	0.0%	0.1%
Pt Birth Date Does Not Match Patient DOB in Database	71	0.1%	3.1%	0.4%
Invalid/Missing Subscriber/Insured ID	72	0.2%	7.8%	0.6%
Invalid/Missing Subscriber/Insured Name	73	0.0%	1.8%	0.0%
Invalid/Missing Subscriber/Insured Gender Code	74	0.0%	0.3%	0.0%
Subscriber/Insured Not Found	75	1.8%	5.3%	9.3%
Duplicate Subscriber/Insured ID Number	76	0.0%	0.0%	0.5%
Subscriber Found, Patient Not Found	77	0.0%	0.6%	0.1%
Subscriber/Insured Not in Group/Plan Identified	78	0.0%	0.0%	0.0%
Other Pt Identification Related Rejection Issues		3.8%	0.0%	0.0%
Rejects due to ***NON ELIGIBILITY RELATED REASONS (e.g., system timeout, provider authorization issues)***		1.7%	1.3%	7.2%
TOTALS		**100.0%**	**100.0%**	**100.0%**
Number of Respondents		**7**	**9**	**3**

3 SCOPE

3.1 What the Rule Applies To

This Phase II CORE rule applies only to certain data elements used to identify a person in loops and data segments in the v5010 270/271 TR3 as specified in §3.4 of this rule.

This Phase II CORE rule defines a standard way to report errors that cause a health plan (or information source) not to be able to respond with a v5010 271 showing eligibility information for the requested patient or subscriber. The goal is to use a unique error code wherever possible for a given error condition so that the re-use of the same error code is minimized. Where this is not possible, the goal (when re-using an error code) is to return a unique combination of one or more AAA segments along with one or more of the submitted patient identifying data elements such that the provider will be able to determine as precisely as possible what data elements are in error and take the appropriate corrective action.

[1] One large national health plan had a significant volume of AAA errors for invalid (not missing) subscriber ID, which resulted in a relatively high overall error rate for this AAA code across all health plans.

3.2 When the Rule Applies

This rule applies only when a health plan (or information source) is processing the data elements identifying an individual in a v5010 270 received from a submitter

and

- the health plan (or information source) performs pre-query evaluation against one or more of the HIPAA-maximum required data elements[2] identifying an individual in a v5010 270 received from a submitter

or

- the health plan (or information source) performs post-query evaluation against one or more of the HIPAA-maximum required data elements identifying an individual in a v5010 270 from a submitter.

In the context of this Phase II CORE rule the following definitions will apply:

- Pre-query evaluation is the logic of one or more checks of the following done by a health plan's (or information source's) system prior to a database look-up to determine if
  - the data elements it requires to identify an individual are present in the v5010 270

or

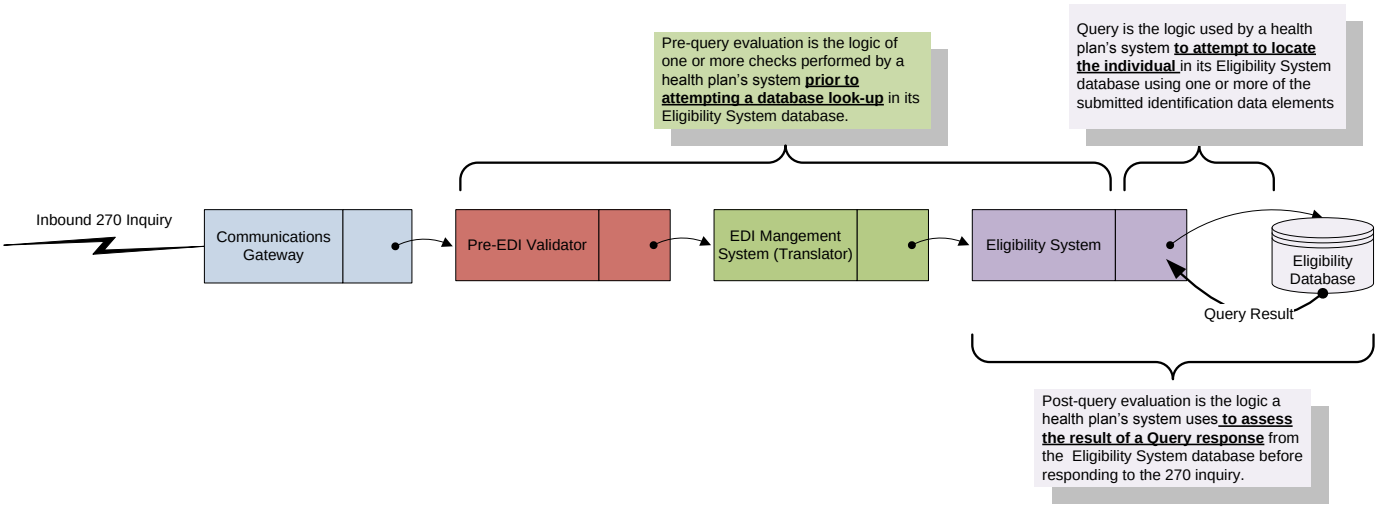
  - the data elements it requires to identify an individual satisfy formatting requirements as defined in §4.3.2 of this rule

or

  - the date-of-birth (DOB) for either the subscriber or dependent is a valid date as defined in §4.3.2 of this rule.
- **Query** is the logic used by a health plan's (or information source's) system to attempt to locate the individual in its eligibility system using one or more of the submitted identification data elements
- **Post-query** evaluation is the logic a health plan's (or information source's) eligibility system uses to assess the results of a Query attempt before responding to the v5010 270.

Figure 1 below is a graphical representation of a conceptual system information flow showing where such pre-query, query and post-query evaluations may take place. This diagram does not represent all systems, but is a conceptual approach solely to illustrate these concepts.

Figure 1 – Conceptual Information Flow



[2] HIPAA-adopted v5010 270/271 TR3 §1.3.8 through §1.4.8.1 specifies the following: "If the patient is the subscriber, the maximum data elements that can be required by an information source to identify a patient in loop 2100C are: Patient's Member ID, Patient's First Name, Patient's Last Name, Patient's Date of Birth. If the patient is a dependent of a subscriber, the maximum data elements that can be required by an information source to identify a patient in loop 2100C and 2100D are: Loop 2100C Subscriber's Member ID, Loop 2100D Patient's First Name, Patient's Last Name, Patient's Date of Birth."

3.3 What the Rule Does Not Require

This Phase II CORE rule does not require a health plan (or information source):

- to use any specific search and match criteria or logic
- to use any specific combination of submitted identification data elements
- to perform a pre-query evaluation
- to perform DOB validation
- to reject the v5010 270 upon detecting an error condition addressed by this rule, but only requires the health plan to return the AAA record when the health plan does reject the v5010 270.

3.4 Applicable Data Elements & Loops

This rule covers the following specified data element and loops in the v5010 270/271 transactions:

Loop ID and Name
Loop 2100C Subscriber Name
Data Element Segment Position, Number & Name
NM103-1035 Last Name
NM104-1036 First Name
NM108-66 ID Code Qualifier
NM109-67 ID Code
DMG02-1251 Subscriber Date of Birth
AAA01-1073 Valid Request Indicator
AAA03-901 Reject Reason Code
AAA04-889 Follow-up Action Code
Loop ID and Name
Loop 2100D Dependent Name
Data Element Segment Position, Number & Name
NM103-1035 Last Name
NM104-1036 First Name
DMG02-1251 Dependent Date of Birth
AAA01-1073 Valid Request Indicator
AAA03-901 Reject Reason Code
AAA04-889 Follow-up Action Code

3.5 Assumptions

- The v5010 270 and v5010 271 are compliant with v5010 270/271 TR3.
- The submitter of the v5010 270 knows which data elements were submitted in the v5010 270 (i.e., member identifier, first name, last name, date of birth).
- A last or first name is considered invalid only when it does not match a last or first name in the health plan's (or information source's) eligibility system.

3.6 Abbreviations Used in this Rule

- MID = member identifier
- FN = first name
- LN = last name
- DOB = date of birth

3.7 Outside the of Scope of this Rule

This rule does not specify whether or not a health plan (or information source) must use the full last or first name or may use only a portion of the last or first name when performing a Pre-Query, Query, or Post-Query process. (Refer to Phase II CORE 258: Normalizing Patient Last Name Rule for use of special characters and letter case in subscriber/patient names.)

4 RULE

4.1 Basic Requirements for Health Plans and Information Sources

A health plan (or information source) is required

- to return a AAA segment for each error condition (as defined in the "Error Condition Description" column of the Error Reporting Codes & Requirements Table in §4.5) that it detects as specified in §4.3 – 4.5

and

- to return code "N" in the AAA01 Valid Request Indicator data element

and

- to return the specified Reject Reason Code in AAA03 as specified in §4.3 – 4.5 for the specific error condition described

and

- to return code "C" in the AAA04 Follow-up Action Code data element

and

- to return data elements submitted and used as specified in §4.5.

This may result in multiple AAA segments being returned in the v5010 271 response such as an AAA segment specifying an error in the LN data element and another AAA segment specifying an error in the MID data element in the same NM1 segment. Examples of such AAA segments include (error conditions and required error codes are specified in subsequent sections of this rule):

AAA*N73*C~**	Indicates LN missing & required or LN does not match LN in eligibility system
AAA*N73*C~**	Indicates FN missing & required or FN does not match FN in eligibility system
AAA*N72*C~**	Indicates MID missing & required or MID does not match MID in eligibility system

4.2 Basic Requirements for Receivers of the v5010 271

The receiver of a v5010 271 (defined in the context of this Phase II CORE rule as the system originating the v5010 270) is required

- to detect all combinations of error conditions from the AAA segments in the v5010 271 as defined in the "Error Condition Description" column of the Error Reporting Codes & Requirements Table in §4.5

and

- to detect all data elements to which this rule applies as returned by the health plan in the v5010 271

and

- to display to the end user text that uniquely describes the specific error condition(s) and data elements returned by the health plan in the v5010 271

and

- ensure that the actual wording of the text displayed accurately represents the AAA03 error code and the corresponding "Error Condition Description" specified in the Error Reporting Codes & Requirements Table in §4.3 – 4.5 without changing the meaning and intent of the error condition description.

The actual wording of the text displayed is at the discretion of the receiver.

4.3 Pre-Query Error Conditions and Reporting Requirements

Pre-query errors may occur when a health plan (or information source) performs various evaluations against the data elements in the v5010 270 used to identify an individual. There are two types of pre-query evaluations that may be performed as specified in §4.3.1 and §4.3.2.

A health plan (or information source) is not required by this rule to perform any pre-query evaluations.

When a health plan (or information source) performs a pre-query evaluation, it must return a AAA segment for each error condition detected along with the data elements submitted and used as specified in §4.3.1 and §4.3.2.

4.3.1 Missing & Required Data Element

This error condition may occur when a health plan (or information source) checks to determine that one or more of the data elements it requires to attempt a database look-up in its eligibility system are present in the submitted v5010 270.

When a health plan (or information source) checks for missing and required data elements and errors are found, the health plan (or information source) is required to return a v5010 271 as specified in §4.5 of this rule.

This rule does not require a health plan (or information source) to check for missing and required data elements.

The maximum data elements that may be required by a health plan (or information source) are specified in §1.3.8 Search Options of the v5010 270/271 TR3.

4.3.2 Invalid MID or DOB

An invalid MID error condition may occur when a health plan (or information source) has specific requirements for the minimum or maximum length or datatype (e.g., all numeric) of a member identifier. This rule does not require a health plan (or information source) to validate a MID for any formatting requirements.

The MID is invalid if it does not meet either the length, formatting or data type requirements of the health plan. When a health plan (or information source) checks the format of the MID and the MID is invalid, the health plan (or information source) must return a v5010 271 as specified in §4.5 of this rule.

An invalid DOB error condition may occur when a health plan (or information source) validates a DOB. This rule does not require a health plan (or information source) to validate a DOB.

A DOB is invalid when it does not represent a valid date as determined by the health plan (or information source).

When a health plan (or information source) validates a DOB and errors are found, the health plan (or information source) is required to return a v5010 271 as specified in §4.5 of this rule.

4.3.3 Pre-Query Error Reporting

When a pre-query error is detected the health plan (or information source) must

- return a AAA segment for each error detected using the appropriate Reject Reason Code for each Pre-Query Error Condition listed in §4.5 of this rule

and

- return the data elements indicated in §4.5 of this rule.

4.4 Post-Query Error Conditions and Reporting Requirements

Post-query errors may occur when a health plan (or information source) attempts a database look-up in its eligibility system and is not able to locate a unique record. The following types of post-query errors that may occur include:

- Look-up attempted, no record found
- Look-up attempted, single record found
- Look-up attempted, multiple records found

The error conditions and error codes reporting requirements tables specified in §4.5 of this rule are designed to apply regardless of a health plan's (or information source's) specific search and match logic. As such, the codes are applicable to any health plan's (or information source's) search and match logic.

A health plan (or information source) is not required by this Phase II CORE rule to use any specific combination of submitted individual identification data elements nor any specific search and match logic.

When a health plan (or information source) detects any of the specified error conditions, it must

- return a AAA segment for each error detected using the appropriate Reject Reason Code for each Post-Query Error Condition as specified in §4.5 of this rule

and

- return the data elements as specified in §4.5 of this rule.

4.5 Error Reporting Codes & Requirements Table

The Error Reporting Codes and Requirements Table below describes each error condition and the corresponding AAA03 error code that must be used to identify the error in the v5010 271. Errors may occur in either the Subscriber Loop or the Dependent Loop or both. The error code that must be used for each defined error condition is marked with an X. The data elements submitted in the v5010 270 that must be returned if used are also specified. Multiple error conditions are possible.

Table 4.5-1 Error Reporting Codes & Requirements Table

Error Reporting Codes & Requirements Table												
		Subscriber Loop							Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)	
		58	71	72	73	76		58	65	71		
Pre-Query - No Look-up Attempted **Missing & Required Data**												
1	Health plan (or information source) requires MID MID was not submitted in the v5010 270 Health plan (or information source) does not attempt look-up			X			None					
2	Health plan requires LN LN was not submitted in the v5010 270 Health plan does not attempt look-up				X		None		X			None
3	Health plan (or information source) requires FN FN was not submitted in the v5010 270 Health plan (or information source) does not attempt look-up				X		None		X			None
4	Health plan (or information source) requires DOB DOB was not submitted in the v5010 270	X					None	X				None

Error Reporting Codes & Requirements Table												
		Subscriber Loop							Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)	
		58	71	72	73	76		58	65	71		
	Health plan (or information source) does not attempt look-up											
Pre-Query – No Look-up Attempted **Formatting Errors**												
5	MID submitted in the v5010 270 does not satisfy health plan (or information source) formatting requirements Health plan (or information source) does not attempt look-up			X			MID submitted					
6	DOB submitted is not valid Health plan (or information source) does not attempt look-up	X					Subscriber DOB submitted	X			DOB submitted at either Subscriber or Dependent Level or both depending on which DOB is in error	
Post-Query – Look-up Attempted **No Record Found**												
7	MID submitted in the v5010 270 in Subscriber loop is not found in eligibility system when health plan (or information source) uses MID to search			X			Subscriber MID submitted Other data elements submitted & used and any AAA error codes associated with these data elements					

Error Reporting Codes & Requirements Table												
		Subscriber Loop							Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)
		58	71	72	73	76		58	65	71	
8	LN submitted in the v5010 270 in Subscriber loop is not found in eligibility system when health plan (or information source) uses LN to search				X		Subscriber LN submitted Other data elements submitted & used and any AAA error codes associated with these data elements				
Post-Query – Look-up Attempted Single Record Found											
9	MID submitted in the v5010 270 in Subscriber loop does not match MID in eligibility system when health plan (or information source) uses LN to search and a single record is returned			X			Subscriber MID submitted Subscriber LN submitted Other data elements submitted & used and any AAA error codes associated with these data elements				
10	LN submitted in the v5010 270 in Subscriber or Dependent loop does not match LN in eligibility system when health plan (or information source) uses MID to search and a single record is returned				X		Subscriber MID submitted Subscriber LN submitted Other data elements submitted & used		X		None
11	FN submitted in the v5010 270 in either Subscriber or Dependent loop does not				X		Subscriber FN submitted Other data elements		X		Dependent FN submitted Other data elements

Error Reporting Codes & Requirements Table											
		Subscriber Loop						Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)
		58	71	72	73	76		58	65	71	
	match FN in eligibility system when health plan (or information source) uses either MID or LN to search and a single record is returned						submitted & used and any AAA error codes associated with these data elements				submitted & used and any AAA error codes associated with these data elements
12	DOB submitted in the v5010 270 in either Subscriber or Dependent loop does not match DOB in eligibility system when health plan (or information source) uses either MID or LN to search and a single record is returned		X				Subscriber DOB submitted Other data elements submitted & used and any AAA error codes associated with these data elements			X	Dependent DOB submitted Other data elements submitted & used and any AAA error codes associated with these data elements
13	LN and/or FN submitted in the v5010 270 in Dependent loop does not match LN and/or FN in eligibility system when health plan (or information source) uses MID to search and a single record is returned *Note: This may be an unlikely condition that could occur, e.g., a MID only submitted in Subscriber loop and Dependent LN submitted*								X		Subscriber MID submitted Other data elements submitted & used and any AAA error codes associated with these data elements

Error Reporting Codes & Requirements Table												
		Subscriber Loop							Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)	
		58	71	72	73	76		58	65	71		
Post-Query Look-up **Multiple Records Found**												
14	Multiple records returned when only a MID submitted in the v5010 270 in Subscriber loop (MID search)					X	Subscriber MID submitted Other data elements submitted & used and any AAA error codes associated with these data elements					
15	Multiple records returned for LN when only LN/FN was submitted in the v5010 270 in Subscriber loop (name search)				X		Subscriber LN submitted Other data elements submitted & used and any AAA error codes associated with these data elements					
16	LN submitted in the v5010 270 in Subscriber loop does not match LN in eligibility system when only LN/MID was submitted and health plan (or information source) uses MID to search and multiple records are returned				X		Subscriber LN submitted Subscriber MID submitted Other data elements submitted & used and any AAA error codes associated with these data elements					
17	FN submitted in the v5010 270 in Subscriber loop does				X		Subscriber FN submitted					

Error Reporting Codes & Requirements Table												
		Subscriber Loop							Dependent Loop			
Error Condition #	Error Condition Description	Invalid/Missing Date-of-Birth	Patient Birth Date Does Not Match That for the Patient in the Database	Invalid/Missing Subscriber/Insured ID	Invalid/Missing Subscriber/Insured Name	Duplicate Subscriber/Insured ID	Data Elements Returned in 271 Response (See Note 1)	Invalid/Missing Date-of-Birth	Invalid/Missing Patient Name	Patient Birth Date Does Not Match That for the Patient in the Database	Data Elements Returned in 271 Response (See Note 1)	
		58	71	72	73	76		58	65	71		
	not match FN in eligibility system when only FN/ LN/MID was submitted and health plan (or information source) uses either MID or LN to search and multiple records are returned						Other data elements submitted & used and any AAA error codes associated with these data elements					

5 CONFORMANCE REQUIREMENTS

Conformance with this rule is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II, the certification testing approach will be similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of a rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the Phase II CORE Certification Test Suite for details.

Table of Contents

1 BACKGROUND SUMMARY

CORE determined that Phase I CORE should focus on improving electronic eligibility and benefits verification, as eligibility is the first transaction in the claims process. Thus, if eligibility and benefits are accurately known to healthcare providers, all the associated electronic transactions that follow will be more effective and efficient. The Phase I CORE 154 Eligibility & Benefits Data Content (270/271) Rule primarily outlined a set of requirements for health plans to return base (not remaining or accumulated) patient financial responsibility related to the deductible, co-pay and co-insurance for a set of 12 services in the HIPAA-adopted ASC X12 005010X279A1 Eligibility Benefit Request and Response (270/271) (hereafter v5010 270/271, v5010 270, v5010 271) transactions, and for vendors, clearinghouse and providers to transmit and use this financial data. The Phase II CORE 260 Eligibility& Benefits (270/271) Data Content Rule extends and enhances the Phase I v5010 271 transaction by requiring the provision of remaining deductible amounts for both the Phase I required 12 Service Type Codes and an additional set of 39 other Service Type Codes.

2 ISSUE TO BE ADDRESSED AND BUSINESS REQUIREMENT JUSTIFICATION

In order to electronically determine a patient's eligibility and benefits, providers need to have a robust v5010 271. This robust response includes the health plans providing financial information, especially remaining deductible amounts, and coverage information for those service types that are heavily used by patients.

HIPAA provides a foundation for the electronic exchange of eligibility and benefits information, but does not go far enough to ensure that today's paper-based system can be replaced by an electronic, interoperable system. HIPAA's current mandated data scope does not require all financial information needed by providers, and HIPAA neither addresses the standardization of data definitions nor contains business requirements by which the HIPAA-outlined data can flow. Future standards developed by ASC X12 and adopted by HIPAA may address these issues. In the meantime, businesses are seeking solutions that can be used today.

Using the available but not-required (situational) elements of the v5010 270/271, the Phase I and II CORE Data Content Rules define the specific business information requirements that health plans must return and vendors, clearinghouses and providers must use if they want to be CORE-certified. As with all CORE rules, these requirements are base requirements, and it is expected many CORE-certified entities will add to these requirements as they work towards the goal of administrative interoperability. This Phase II CORE 260 Eligibility & Benefits Data Content (270/271) Rule requires the delivery of the remaining deductible amount (in addition to base contract deductible amount, which is required in Phase I), outlines how a health plan deductible vs. a benefit or service type-specific deductible is to be specified in the v5010 271, and provides an expanded list of CORE-required service type codes, which are additions to the 12 Service Type Codes that the Phase I CORE 154 Eligibility & Benefits (270/271) Data Content Rule requires.

By requiring the delivery and use of this financial information via the existing v5010 270/271 HIPAA-adopted standard, the Phase II CORE 260 Eligibility & Benefits (270/271) Data Content Rule helps provide the information that is necessary to more fully automate electronic eligibility and benefits inquiry processes and thus reduce the cost of today's more manual processes. Moreover, to ensure industry coordination, the Phase I and Phase II CORE 154/260 Eligibility & Benefits (270/271) Data Content Rules take into consideration many of the requirements included in the ASC X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 (TR3) (hereafter v5010 TR3) implementation guide, thus enabling the industry to realize many of these benefits now.

3 SCOPE

3.1 What the Rule Applies To

This CORE rule conforms with and builds upon the ASC X12 005010X279A1 Health Care Eligibility Benefit Inquiry and Response (270/271) Technical Report Type 3 (TR3) implementation guide specifies the minimum content that a CORE-certified entity must include in the v5010 271.

This rule builds upon and extends the Phase I CORE 154 Eligibility& Benefits (270/271) Data Content Rule Version 1.1.0 by addressing ambiguities, extending requirements and adding CORE constraints to the v5010 271 content that a CORE-certified entity must include in the v5010 271 (See §3.6.1.).

3.2 When the Rule Applies

This rule applies when:

- The individual is located in the health plan's (or information source's) eligibility system

And

- A health plan (or information source) receives a generic v5010 270;

Or

- A health plan (or information source) receives an explicit v5010 270 for a specific service type required in §4.1.1.1 of this rule.

3.3 What the Rule Does Not Require

This rule does not require any CORE-certified entity to modify its use and content of:

- Other loops and data elements that may be submitted in the v5010 270 not addressed in this rule (see §3.4)

And

- Other loops and data elements that may be returned in the v5010 271 not addressed in this rule (see §3.4).

3.4 Applicable Loops & Data Elements

This rule covers the following specified loops, segments and data elements in the v5010 270/271 transactions:[1]

In the v5010 270:

- Loop 2110C Subscriber Eligibility or Benefit Inquiry Information
  - EQ Subscriber Eligibility or Benefit Inquiry Information Segment
- Loop 2110D Dependent Eligibility or Benefit Inquiry Information
  - EQ Dependent Eligibility or Benefit Inquiry Information Segment

In the v5010 271:

- Loop 2100C Subscriber Name
  - DTP01-374 Date/Time Qualifier
  - DTP02-1250 Date Time Period Format Qualifier
  - DTP03-1251 Date Time Period
- Loop 2110C Subscriber Eligibility or Benefit Information
  - EB01-1390 Eligibility or Benefit Information
  - EB02-1207 Coverage Level Code
  - EB03-1365 Service Type Code
  - EB06-615 Time Period Qualifier
  - EB07-782 Monetary Amount
  - EB08-954 Percent
  - EB12-1073 Yes/No – In Plan Network Indicator
  - DTP01-374 Date/Time Qualifier
  - DTP02-1250 Date Time Period Format Qualifier

[1] Loops, segments and data elements in normal font are addressed in Phase I CORE 154 Eligibility & Benefits 270/271 Data Content Rule Version 1.1.0 and any subsequent versions. Loops, segments and data element in bold font are addressed only in this CORE Phase II Data Content Rule.

- DTP03-1251 Date Time Period

- Loop 2100D Dependent Name
  - DTP01-374 Date/Time Qualifier
  - DTP02-1250 Date Time Period Format Qualifier
  - DTP03-1251 Date Time Period
- Loop 2110D Dependent Eligibility or Benefit Information
  - EB01-1390 Eligibility or Benefit Information
  - EB02-1207 Coverage Level Code
  - EB03-1365 Service Type Code
  - EB06-615 Time Period Qualifier
  - EB07-782 Monetary Amount
  - EB08-954 Percent
  - EB12-1073 Yes/No – In-Plan Network Indicator
  - DTP01-374 Date/Time Qualifier
  - DTP02-1250 Date Time Period Format Qualifier
  - DTP03-1251 Date Time Period

3.5 Outside the Scope of this Rule

This rule does not:

Require CORE-certified entities to internally store the data elements listed in §3.4 or any other data elements in conformance with this rule, but rather requires that all CORE-certified entities conform to this rule when conducting the v5010 270/271 transactions electronically. Entities may store data internally any way they wish, but must ensure the data conform to applicable CORE rules when inserting that data into outbound transactions.

3.6 Assumptions

The following assumptions apply to this rule:

- This rule is a component of the larger set of Phase II CORE rules; as such, all the CORE Guiding Principles apply to this rule and all other rules.
- All entities seeking Phase II certification must be Phase I certified as Phase I CORE provides a foundation for Phase II CORE.
- Requirements for the use of the applicable loops and data elements apply only to the v5010 270/271.
- Health plans (and information sources) are able to accurately maintain benefit and eligibility data received or created in a reasonable timeframe.
- The terms used in this rule are defined in §3.7 and in the Phase II CORE Glossary of Data Content Terms, which is an Appendix to this rule.
- This rule is not a comprehensive companion document specifying the complete content of either the v5010 270 or v5010 271 transactions. The focus in this rule is on specifying requirements for the v5010 271 to address the Phase II CORE data content requirements for health plan benefits and services and related patient financial responsibility.

3.6.1 Builds on Phase I Eligibility and Benefits Data Content v5010 270/271 Rule

This rule builds upon and extends the Phase I CORE 154 Eligibility & Benefits Data Content (270/271) Rule Version 1.1.0 by addressing ambiguities, extending requirements and adding new CORE constraints to the v5010 271 content of the v5010 271 transaction.

Given that any entity seeking Phase II certification will need to be Phase I certified (see Phase II CORE Guiding Principles) and because the Phase II Data Content rule is built upon the Phase I Data Content Rule, the Phase II Data Content rule incorporates by reference all the requirements of the Phase I CORE 154 Eligibility & Benefits Data Content (270/271) Rule Version 1.1.0.

3.7 Abbreviations and Definitions Used in this Rule

Health Plan Base Deductible: *The dollar amount of covered services based on the allowed benefit that must be paid by an individual or family per benefit period before the health benefit plan begins to pay its portion of claims. The benefit period may be a specific date range of one year or other as specified in the plan. (See the entry for Health Plan Deductible in the Phase II CORE Glossary of Data Content Terms.)*

Benefit-specific Base Deductible*: The dollar amount of a specific covered service based on the allowed benefit that is separate and distinct from the Health Plan Base Deductible that must be paid by an individual or family before the health benefit plan begins to pay its portion of claims. The specific benefit period may be a specific date, date range, or otherwise as specified in the plan.*

Explicit Inquiry: *In contrast to a Generic Inquiry, an Explicit Inquiry is a v5010 270 Health Care Eligibility Benefit Inquiry that contains a Service Type Code other than and not including "30" (Health Benefit Plan Coverage) in the EQ01 segment of the transaction. An Explicit Inquiry asks about coverage of a specific type of benefit, for example, "78" (Chemotherapy). (See* ***§****4.1.1.1.)*

Generic Inquiry: *In contrast to an Explicit Inquiry, a Generic Inquiry is a v5010 270 Health Care Eligibility Benefit Inquiry that contains only Service Type Code "30" (Health Benefit Plan Coverage) in the EQ01 segment of the transaction.*

Health Plan Coverage Date for the Individual: *The effective date of health plan coverage actually in operation and in force for the individual.*

Support [Supported] Service Type: *Support [or Supported] means that the health plan (or information source) must have the capability to receive a v5010 270 inquiry for a specific Service Type Code and to respond in the corresponding v5010 271 response in accordance with this rule.*

Other terms and concepts used in this rule are defined in the Phase II CORE Glossary of Data Content Terms, which is an Appendix to this rule.

4 RULE

4.1 Basic Requirements for Health Plans and Information Sources

A CORE Phase II-certified health plan (or information source) is required to comply with all requirements specified in this rule when returning the v5010 271 when the individual is located in the health plan's (or information source's) system.

4.1.1 Specifying Health Benefits Coverage

4.1.1.1 Requirements for a Response to an Explicit Inquiry for a CORE Required Service Type

A CORE-certified health plan (or information source) must support an explicit v5010 270 for each of the CORE service types specified in Table 4.1.1.1 by returning a v5010 271 as specified in §4.1.2 through §4.1.5.

Table 4.1.1.1 specifies 51 Service Type Codes, 12 of which are required in the Phase I CORE Rule. These 12 required service types specified in Phase I CORE 154 Eligibility & Benefits (270/271) Data Content Rule are included in this Phase II rule by reference and are identified in Table 4.1.1.1 in italic font.

TABLE 4.1.1.1 CORE REQUIRED SERVICE TYPES FOR AN EXPLICIT INQUIRY	
CORE REQUIRED EXPLICIT INQUIRY SERVICE TYPES (v5010 X12 270/271 Code and Definition)	**CORE SUPPLEMENTAL DESCRIPTION[2]**
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 healthcare professionals.*
2 Surgical	footnote 2
4 Diagnostic X-Ray	footnote 2
5 Diagnostic Lab	footnote 2
6 Radiation Therapy	footnote 2
7 Anesthesia	footnote 2
8 Surgical Assistance	Assistant Surgeon/surgical assistance provided by a physician if required because of the complexity of the surgical procedures.
12 Durable Medical Equipment Purchase	Purchase of medically necessary equipment and supplies prescribed by a physician or other healthcare provider that can withstand repeated use, is medically necessary for the patient, is not useful if the patient is not ill or injured, and can be used in the home.
13 Ambulatory Service Center Facility	A freestanding facility that provides services on an outpatient basis, primarily for the purpose of performing medical or surgical procedures.
18 Durable Medical Equipment Rental	Rental of medically necessary equipment and supplies prescribed by a physician or other healthcare provider that can withstand repeated use, is medically necessary for the patient, is not useful if the patient is not ill or injured, and can be used in the home.
20 Second Surgical Opinion	footnote 2
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.*
40 Oral Surgery	footnote 2
42 Home Health Care	footnote 2
45 Hospice	footnote 2
47 Hospital	footnote 2
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.*
51 Hospital - Emergency Accident	Hospital services and supplies for the treatment of a sudden and unexpected injury that requires immediate medical attention.
52 Hospital - Emergency Medical	Hospital services and supplies for the treatment of a sudden and unexpected condition that requires immediate medical attention.
53 Hospital - Ambulatory Surgical	footnote 2
62 MRI/CAT Scan	footnote 2
65 Newborn Care	footnote 2
68 Well Baby Care	footnote 2
73 Diagnostic Medical	footnote 2

[2] The CORE supplemental descriptions (clarification/meaning) are for guidance until definitive clarified definitions can be obtained within the ASC X12 standards. They provide a general understanding of the specific services which are included in each service type, but the description may not be all inclusive. No CORE description is provided for Service Type Codes where there was agreement among the CORE participants that the ASC X12 Standard Code Definition is sufficiently clear and commonly understood.

TABLE 4.1.1.1 CORE REQUIRED SERVICE TYPES FOR AN EXPLICIT INQUIRY	
CORE REQUIRED EXPLICIT INQUIRY SERVICE TYPES (v5010 X12 270/271 Code and Definition)	**CORE SUPPLEMENTAL DESCRIPTION[2]**
76 Dialysis	footnote 2
78 Chemotherapy	footnote 2
80 Immunizations	footnote 2
81 Routine Physical	footnote 2
82 Family Planning	footnote 2
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.*
93 Podiatry	footnote 2
98 Professional (Physician) Visit - Office	footnote 2
99 Professional (Physician) Visit - Inpatient	footnote 2
A0 Professional (Physician) Visit - Outpatient	footnote 2
A3 Professional (Physician) Visit - Home	footnote 2
A6 Psychotherapy	footnote 2
A7 Psychiatric - Inpatient	footnote 2
A8 Psychiatric - Outpatient	footnote 2
AD Occupational Therapy	footnote 2
AE Physical Medicine	footnote 2
AF Speech Therapy	footnote 2
AG Skilled Nursing Care	Services and supplies for a patient who has been admitted to a skilled nursing facility for the purpose of receiving medical care or other health services.
AI Substance Abuse	footnote 2
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.*
BG Cardiac Rehabilitation	footnote 2
BH Pediatric	footnote 2
MH Mental Health	footnote 2
UC Urgent Care	footnote 2

4.1.2 Specifying Status of Health Benefits Coverage

For the discretionary Service Type Codes identified in §4.1.3, when the health plan is exercising its discretion to not return patient financial responsibility, the status of the specific benefit (service type) must be returned regardless of whether or not that status is separate and distinct from the status of the health plan coverage.

When a service type covered by this rule is a covered benefit for in-network providers only and not a covered benefit for out-of-network providers, a CORE-certified health plan (or information source) must indicate the non-

covered status for out-of-network providers for each service type using EB12-1073 Yes/No – In Plan Network Indicator as follows:

EB01 = I−Non Covered

EB03 = <Applicable Service Type Code>

EB12 = N

4.1.3 Patient Financial Responsibility

A CORE-certified health plan (or information source) must return the patient financial responsibility for base and remaining deductible, co-insurance and co-payment as specified in §4.1.3.1 through §4.1.3.3 for each of the service type codes returned. The health plan (or information source) may, at its discretion, elect not to return patient financial responsibility information (deductible, co-payment or co-insurance) for the following Service Type Codes specified in EB03-1365:

- 1 – Medical Care;
- 35 – Dental Care;
- 88 – Pharmacy;
- A6 – Psychotherapy;
- A7 – Psychiatric – Inpatient;
- A8 – Psychiatric – Outpatient;
- AI – Substance Abuse; and
- AL – Vision (Optometry);
- MH – Mental Health.

This discretionary reporting of patient financial responsibility information does not preempt the health plan's (or information source's) requirement to report patient financial responsibility for deductible, co-payment and co-insurance for all other Service Type Codes as specified in Table 4.1.1.1.

Service Type Code 30−Health Benefit Plan Coverage is not included in this group of discretionary service types since this rule requires that a CORE-certified health plan (or information source) must return base and remaining Health Plan Deductibles using Service Type Code 30.

CORE made these codes discretionary for one of three main reasons:

- A code is too general for a response to be meaningful (e.g., 1 – Medical), especially given the new specific codes added in Phase II;
- A code is typically a "carve-out" benefit (e.g., AL – Vision) where the specific benefit information is not available to the health plan or information source; or
- A code is related to behavioral health or substance abuse (e.g., AI - Substance Abuse) where privacy issues may impact a health plan or information source's ability to return information.

See §6.1 Appendix 1 for a visual view of Service Type Codes and reporting requirements.

All date and date range reporting requirements for Patient Financial Responsibility are specified in §4.1.4.

4.1.3.1 Specifying Deductible Amounts

A CORE-certified health plan (or information source) must return the dollar amount of the base and remaining deductible for all Service Type Codes required by §4.1.1.1 and for Service Type Code 30 (See §4.1.1.1.), with consideration of §4.1.3 for discretionary reporting exceptions.

The deductible amount returned must be in U.S. dollars only.

4.1.3.1.1 Specifying the Health Plan Base Deductible

A CORE-certified health plan (or information source) must return the Health Plan base deductible as defined in §3.7 of this rule that is the patient financial responsibility, including both individual and family deductibles (when

applicable) in Loops 2110C/2110D only when the status of the health plan coverage as required in §4.1.2 is equal to one of the active coverage codes 1 through 5 and EB03=30 – Health Benefit Plan Coverage as follows:

EB01 = C–Deductible

EB02 = FAM–Family or IND–Individual as appropriate

EB03 = 30 – Health Benefit Plan Coverage

EB06 = <Applicable Time Period Qualifier code; see Table 4.1.3.1.1 for recommended qualifiers.>

EB07 = Monetary amount of Health Plan base deductible

TABLE 4.1.3.1.1 CORE Recommended Time Period Qualifier Codes	
CORE RECOMMENDED TIME PERIOD QUALIFIER CODES (v5010 X12 270/271 Code and Definition)	**CORE SUPPLEMENTAL DESCRIPTION[3]**
22 Service Year	A 365-day (366 in leap year) period. This period may not necessarily be a Calendar Year (for example April 1 through March 31).
23 Calendar Year	January 1 through December 31 of the same year.
25 Contract	The duration of the patient's specific coverage with the health plan.

When a service type does not have a base deductible separate and distinct from the Health Plan base deductible, the Health Plan base deductible must not be returned on any EB segment where EB03≠30 − Health Benefit Plan Coverage.

When the Health Plan base deductible differs for in- and out-of-network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as follows:

EB12 = N or Y as applicable

4.1.3.1.2 Specifying the Health Plan Remaining Deductible

A CORE-certified health plan (or information source) must return the Health Plan remaining deductible as defined in the Phase II CORE Glossary of Data Content Terms, which is an Appendix to this rule, that is the patient financial responsibility, including both individual and family remaining deductibles (when applicable) in Loops 2110C/2110D only when the status of the health plan coverage as required in §4.1.2 is equal to one of the active coverage codes 1 through 5 and EB03=30 – Health Benefit Plan Coverage as follows:

EB01 = C–Deductible

EB02 = FAM–Family or IND–Individual as appropriate

EB03 = 30 – Health Benefit Plan Coverage

EB06 = 29–Remaining

EB07 = Monetary amount of Health Plan remaining deductible

When a service type does not have a specific remaining deductible that is separate and distinct from the Health Plan remaining deductible, the Health Plan remaining deductible must not be returned on any EB segment where EB03≠30−Health Benefit Plan Coverage.

When the Health Plan remaining deductible differs for in- and out-of-network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as follows.

EB12 = N or Y as applicable

[3] CORE descriptions (clarification/meaning) provide a more explicit understanding of the specific time period applicable to the health plan deductible amounts.

The Health Plan remaining deductible returned is for the current time period only, i.e., as of the date of the v5010 271. When the v5010 270 is for a time period other than the current time period, no Health Plan remaining deductible is returned.

4.1.3.1.3 Specifying the Benefit-specific Base Deductible

A CORE-certified health plan (or information source) must return the Benefit-specific base deductible as defined in §3.7 of this rule that is the patient financial responsibility, including both individual and family deductibles (when applicable) in Loops 2110C/2110D only when the status of the health plan coverage and the status of the specific benefit as required in §4.1.2 is equal to one of the active coverage codes 1 through 5 and EB03≠30–Health Benefit Plan Coverage as follows:

EB01 = C–Deductible

EB02 = FAM–Family or IND–Individual as appropriate

EB03 = <the Service Type Code indicating the specific benefit to which the deductible applies>

EB06 = <Applicable Time Period Qualifier code; see Table 4.1.3.1.1 for recommended qualifiers.>

EB07 = Monetary amount of Benefit-specific base deductible

When the Benefit-specific base deductible differs for in- and out-of-network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as follows:

EB12 = N or Y as applicable

4.1.3.1.4 Specifying the Benefit-specific Remaining Deductible

A CORE-certified health plan (or information source) must return the Benefit-specific remaining deductible as defined in the Phase II CORE Glossary of Data Content Terms, which is an Appendix to this rule, that is patient financial responsibility, including both individual and family deductibles (when applicable) in Loops 2110C/2110D only when the status of the health plan coverage and the status of the specific benefit as required in §4.1.2 is equal to one of the active coverage codes 1 through 5 and EB03≠30–Health Benefit Plan Coverage as follows:

EB01 = C–Deductible

EB02 = FAM–Family or IND–Individual as appropriate

EB03 = <the Service Type Code indicating the specific benefit to which the deductible applies>

EB06 = 29 – Remaining

EB07 = Monetary amount of Benefit-specific remaining deductible

When the Benefit-specific remaining deductible differs for in- and out-of-network, two occurrences of the EB segment must be returned using EB12-1073 with codes N and Y as follows:

EB12 = N or Y as applicable

The benefit-specific remaining deductible returned is for the current time period only, i.e., as of the date of the v5010 271. When the v5010 270 is for a time period other than the current time period, no Benefit-specific remaining deductible is returned.

Returning the Benefit-specific remaining deductible is required except for those service types specified as exceptions for discretionary reporting in §4.1.3.

4.1.3.2 Specifying Co-Payment Amounts

A CORE-certified health plan (or information source) must return the patient financial responsibility for co-payment for each of the Service Type Codes returned as specified as follows:

EB01 = B–Co-Payment

EB02 = FAM–Family or IND–Individual as appropriate

EB07 = Monetary amount of Benefit-specific Co-payment

When 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 follows:

EB12 = N or Y as applicable

See §4.1.3 for discretionary reporting exceptions.

4.1.3.3 Specifying Co-Insurance Amounts

A CORE-certified health plan (or information source) must return the patient financial responsibility for co-insurance for each of the Service Type Codes returned as follows:

EB01 = A–Co-Insurance

EB02 = FAM–Family or IND–Individual as appropriate

EB08 = Percent for each Benefit-specific Co-insurance

When 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 follows:

EB12 = N or Y as applicable

See §4.1.3 for discretionary reporting exceptions.

4.1.4 Specifying the Health Plan Base Deductible Dates

When the Health Plan Base Deductible date is not the same date as the Health Plan Coverage Date for the Individual a CORE-certified health plan (or information source) must return date specifying the begin date for the base Health Plan deductible only in Loops 2110C/2110D where EB01= active coverage code 1 through 5 and EB03=30–Health Plan Benefit Coverage and EB01=C−Deductible as follows:

DTP01 = 346 Plan Begin

DTP02 = D8–Date Expressed in Format CCYYMMDD

DTP03 = the date applicable to the time period as specified in EB06

Do not return the DTP segment when the date is the same as the Health Plan Coverage Dates for the Individual.

Alternatively, a CORE-certified health plan (or information source) may return a range of dates specifying the begin and end dates for the base Health Plan Base deductible only in Loops 2110C/2110D where EB01 = active coverage code 1 through 5 and EB03=30–Health Plan Benefit Coverage and EB01 = C−Deductible as follows:

DTP01 = 291–Plan

DTP02 = RD8–Date Expressed in Format CCYYMMDD-CCYYMMDD

DTP03 = the range of dates applicable to the time period as specified in EB06

Do not return the DTP segment when the date range is the same as the Health Plan Coverage Dates for the.

4.1.5 Specifying Benefit-specific Base Deductible Dates

When the Benefit-specific Base Deductible date is not the same date as the Health Plan Coverage Dates for the Individual, a CORE-certified health plan (or information source) must return a date specifying the begin date for the base Benefit-specific deductible only in Loops 2110C/2110D where EB01= active coverage code 1 through 5 and EB03≠30–Health Plan Benefit Coverage and EB01=C−Deductible as follows:

DTP01 = 348–Benefit Begin

DTP02 = D8–Date Expressed in Format CCYYMMDD

DTP03 = the date applicable to the time period as specified in EB06

Do not return the DTP segment when the date is the same as the Health Plan Coverage Dates for the Individual.

Alternatively, a CORE-certified health plan (or information source) may return a range of dates specifying the begin and end dates for the base Benefit-specific deductible only in Loops 2110C/2110D where EB01= active coverage code 1 through 5 and EB03≠30–Health Plan Benefit Coverage and EB01=C−Deductible as follows:

DTP01 = 292–Benefit

DTP02 = RD8–Date Expressed in Format CCYYMMDD-CCYYMMDD

DTP03 = the range of dates applicable to the time period as specified in EB06

Do not return the DTP segment when the date range is the same as the Health Plan Coverage Dates for the Individual.

4.2 Basic Requirements for Submitters (Providers, Provider Vendors and Information Receivers)

The receiver of a v5010 271 (defined in the context of this CORE rule as the system originating the v5010 270) is required to detect and extract all data elements to which this rule applies as returned by the health plan (or information source) in the v5010 271.

The receiver must display or otherwise make the data appropriately available to the end user without altering the semantic meaning of the v5010 271 data content.

5 CONFORMANCE REQUIREMENTS

Conformance with this rule is considered achieved when all of the required detailed step-by-step test scripts specified in the Phase II CORE Certification Test Suite are successfully passed.

For Phase II Data Content, the certification testing approach will be similar to the Phase I testing approach. In Phase I, entities were not tested for their compliance with all sections of the Data Content rule, rather just certain sections as testing is not exhaustive and is paired with the CORE Enforcement policy. CORE certification requires entities to be compliant with all aspects of the rule when working with all trading partners, unless the CORE-certified entity has an exemption. Refer to the CORE Certification Test Suite for details.

6 APPENDIX

The purpose of the Appendix is to provide additional background on the Phase II CORE Data Content rule. It is non-normative information and in a case of conflict, the actual rule language applies.

6.1 Appendix 1: Phase II CORE Service Type Codes

Appendix 1 shows the full list of Service Type Codes required in Phase II CORE. It includes the generic code 30 (Health Benefit Plan Coverage) and the twelve specific codes required in the Phase I CORE 154 Eligibility & Benefits (270/271) Data Content Rule. Phase II adds 39 additional Service Type Codes required to be supported for explicit inquiries. The Phase I Service Type Codes appear as green-shaded boxes. In Phase II these twelve Service Type Codes continue to be required for a v5010 271 response to a generic v5010 270 (Code 30 request).

Phase II continues the discretionary reporting of patient financial responsibility for five of the Phase I Service Type Codes and adds four of the 39 new Phase II Service Type Codes to the list of service types for which patient financial responsibility reporting is discretionary.

The right-hand column describes the required and discretionary status for returning patient financial responsibility information (static co-pay and co-insurance information and remaining deductible amount) for each of the 52 Service Type Codes in Phase II, including Service Type Code 30 – Health Benefit Plan Coverage.

Expanded Subset of Service Type Codes for Phase II (X12 270/271 Code and Definition)	Service Type Codes Required for a Generic Inquiry	Service Type Codes Required for an Explicit Inquiry	Return patient financial responsibility information (static co-pay and co-insurance information and remaining deductible amount)?
1 Medical Care	Y	Y (Phase I)	**Discretionary**
2 Surgical		Y	Mandatory
4 Diagnostic X-Ray		Y	Mandatory
5 Diagnostic Lab		Y	Mandatory
6 Radiation Therapy		Y	Mandatory
7 Anesthesia		Y	Mandatory
8 Surgical Assistance		Y	Mandatory
12 Durable Medical Equipment Purchase		Y	Mandatory
13 Ambulatory Service Center Facility		Y	Mandatory
18 Durable Medical Equipment Rental		Y	Mandatory
20 Second Surgical Opinion		Y	Mandatory
30 Health Benefit Plan Coverage	Y		Mandatory
33 Chiropractic	Y	Y (Phase I)	Mandatory
35 Dental Care	Y	Y (Phase I)	**Discretionary**
40 Oral Surgery		Y	Mandatory
42 Home Health Care		Y	Mandatory
45 Hospice		Y	Mandatory
47 Hospital	Y	Y (Phase I)	Mandatory
48 Hospital - Inpatient	Y	Y (Phase I)	Mandatory
50 Hospital - Outpatient	Y	Y (Phase I)	Mandatory
51 Hospital - Emergency Accident		Y	Mandatory
52 Hospital - Emergency Medical		Y	Mandatory
53 Hospital - Ambulatory Surgical		Y	Mandatory
62 MRI/CAT Scan		Y	Mandatory
65 Newborn Care		Y	Mandatory
68 Well Baby Care		Y	Mandatory
73 Diagnostic Medical		Y	Mandatory
76 Dialysis		Y	Mandatory
78 Chemotherapy		Y	Mandatory
80 Immunizations		Y	Mandatory
81 Routine Physical		Y	Mandatory
82 Family Planning		Y	Mandatory
86 Emergency Services	Y	Y (Phase I)	Mandatory
88 Pharmacy	Y	Y (Phase I)	**Discretionary**
93 Podiatry		Y	Mandatory
98 Professional (Physician) Visit - Office	Y	Y (Phase I)	Mandatory
99 Professional (Physician) Visit - Inpatient		Y	Mandatory
A0 Professional (Physician) Visit - Outpatient		Y	Mandatory
A3 Professional (Physician) Visit - Home		Y	Mandatory
A6 Psychotherapy		Y	**Discretionary**
A7 Psychiatric - Inpatient		Y	**Discretionary**
A8 Psychiatric - Outpatient		Y	**Discretionary**
AD Occupational Therapy		Y	Mandatory
AE Physical Medicine		Y	Mandatory
AF Speech Therapy		Y	Mandatory
AG Skilled Nursing Care		Y	Mandatory
AI Substance Abuse		Y	**Discretionary**
AL Vision (Optometry)	Y	Y (Phase I)	**Discretionary**
BG Cardiac Rehabilitation		Y	Mandatory
BH Pediatric		Y	Mandatory
MH Mental Health	Y	Y (Phase I)	**Discretionary**
UC Urgent Care	Y	Y (Phase I)	Mandatory

6.2 Appendix 2: Glossary of Data Content Terms

The glossary is advisory only and is available for download from the CAQH Web site.

Table of Contents

REVISION HISTORY FOR PHASE II CORE CONNECTIVITY RULE

Version	Revision	Description	Date
2.0.0	Major	CORE Phase II Connectivity Rule, balloted and approved by CORE members.	July 15, 2008
2.0.1	Minor	Batch connectivity schemas and examples have been updated to eliminate gaps identified by early adopters.	Mar 16, 2009
Change Summary for Version 2.0.1 1. Section 4.2.1.3 • Removed "Request" from "Batch Submission Request Message Structure" specification title 2. Section 4.2.1.4 • Specification added 3. Section 4.2.1.5 - 4.2.1.6 • Original Batch Submission Acknowledgment Message Structure specification subdivided 4. Section 4.2.1.7 - 4.2.1.8 • "Results" added to specification titles 5. Section 4.2.1.9 - 4.2.1.10 • Specifications added 6. Section 4.2.2.5 • Removed "Request" from "Batch Submission Request Message Structure" specification title 7. Section 4.2.2.6 • Specification added 8. Section 4.2.2.7 - 4.2.2.8 • Original Batch Submission Acknowledgment Message Structure specification subdivided 9. Section 4.2.2.9 - 4.2.2.10 • "Results" added to specification titles 10. Section 4.2.1.11 - 4.2.1.12 • Specifications added 11. Section 6.3.1 • Real time interaction sequence diagram added 12. Section 6.3.2 • Batch interaction sequence diagram added			
2.2.0	Minor	1. Adjustments to support ASC X12 HIPAA-adopted v5010 Eligibility and Claim Status transactions to support PPACA Section 1104 2. Revisions to address Phase II FAQs 3. Updates to the SOAP+WSDL and HTTP+MIME examples to correct errors and omissions and to make the examples consistent with updated PayloadTypes table 4. Adjustments to optional and required field inconsistencies as described in the metadata table in the Connectivity Rule, as specified in the SOAP XSD schema and as presented in the examples for SOAP and/or HTTP+MIME under Schemas, Examples and Rule Text 5. MIME examples in Sections 4.2.1.1 through 4.2.1.9 were corrected to remove the filename attribute, which is not addressed by the CORE rule 6. Section 4.3.4.1 modified by removing the requirement for HTTP Header Date field, an incorrect holdover of text from previous rule version 7. MIME Examples in Sections 4.2.1.3 through 4.2.1.10 and SOAP Examples in Sections 4.2.2.5 through 4.2.2.12 updated to show MIME and SOAP examples using only ASC X12 270/271 payload type values rather than mixed batch payload type values 8. Section 6.3.2 expanded to show a new sequence diagram for specific payload types in addition to the Mixed Payload Type sequence interaction diagram that already exist	Mar 18, 2011

1 BACKGROUND

This rule addresses the message envelope metadata, the message envelope standards and the submitter authentication standards for both batch and real time transactions, and communications-level errors and acknowledgements. This rule is designed to provide a "safe harbor" that the 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.

1.1 Guiding Principles

The following CORE guiding principles apply to the CORE Phase II Connectivity Rule:

- CORE will not create or promote proprietary approaches to electronic interactions/transactions.
- CORE will suggest migration steps to promote successful and timely adoption of CORE rules.
- To promote interoperability, rules will be built upon HIPAA, and CORE will coordinate with other key industry bodies (for example, ASC 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).
- CORE will not build a switch, database, or central repository of information.
- All CORE recommendations and rules will be vendor neutral.
- Rules will not be based on the least common denominator but rather will encourage feasible Phase II progress.
- CORE will promote and encourage voluntary adoption of the rules.
- CORE participants do not support "phishing."
- CORE rules address both *Batch* and *Real time* (these terms are defined in *Appendix 6.1: Abbreviations and Definitions used in this Rule*), with a movement towards Real time (Hence, Phase II certification related to batch does not apply to entities that do not do batch transactions.)
- All of the Phase II rules are expected to evolve in future phases.
- CORE's Connectivity rules are written such that they can accommodate not only Eligibility transactions, but also can apply to any other administrative transaction.
- Acknowledging connectivity support for Eligibility, Claim Status and other administrative transactions in light of the Patient Protection and Affordable Care Act (ACA) §1104.

2 ISSUES TO BE ADDRESSED AND BUSINESS JUSTIFICATION

Currently, multiple connectivity methods – some based on open standards, others on proprietary approaches – are in use for administrative electronic transactions in the healthcare industry. Healthcare providers and health plans support multiple connectivity methods to connect to different health plans, clearinghouses, provider organizations and others. Supporting multiple connectivity methods for administrative electronic transactions adds costs for health plans and providers. Connectivity and Security standards from standards development organizations such as OASIS, W3C, and IETF are intended to be industry neutral, allowing for implementation variations, and thus are not specific enough to provide interoperability in healthcare. For example, several open standards for enveloping, such as SOAP and ebMS exist in the marketplace. These open standards are industry neutral and hence do not define the metadata, vocabularies and semantics needed to support industry specific transactions. Further complicating this issue is the wide variance in

implementations of these standards in the healthcare market, the continuing use of proprietary approaches and the industry's developing use of the public internet.

The Committee on Operating Rules for Information Exchange (CORE®) Connectivity & Security Subgroup aims to fill this gap by adopting existing open standards and formulating Connectivity/Security Rules that provide industry specific (i.e., for healthcare administrative electronic transactions) guidance on using these open standards. The CORE Connectivity Rule was developed using a consensus-based approach among industry stakeholders, and is designed to facilitate interoperability, improve utilization of administrative transactions, enhance efficiency and lower the cost of information exchange in healthcare.

The following sections describe the work completed while developing the CORE Phase I Connectivity Rule, and the outstanding issues that are being addressed by the CORE Phase II Connectivity Rule. The rationale for the selected envelope and authentication standards within the CORE Phase II Connectivity Rule is also presented.

2.1 CORE Phase II Connectivity Rule Background

CORE Phase I (i.e., *CORE Operating Rule 153: Connectivity Rule*) defined a Connectivity/Security Rule, which is a safe harbor that required the use of the HTTP/S transport protocol over the public Internet. It also specified a minimum set of metadata outside the ASC X12 payload (e.g., date/time, payload ID, and other elements), and aspects of connectivity/security such as response times, acknowledgements and errors. Since the CORE Phase I Connectivity Rule is a safe harbor, CORE Phase I-certified entities are required to support the adopted CORE Phase I Connectivity method at a minimum, but may also implement additional other connectivity/security methods. A set of Conformance Tests were defined for CORE Phase I Connectivity certification and many organizations have attained CORE Phase I certification.

The CORE Phase I Connectivity Rule (i.e., *CORE Operating Rule 153: Connectivity Rule*) required the use of HTTP/S over the public Internet. CORE made a decision to limit the rule at this high-level to provide a first step toward Connectivity, understanding that later phases of CORE would issue more detailed requirements. CORE was aware the Phase I Rule did not provide the optimum level of specificity for implementations as it was developed as a first step. CORE Phase I Connectivity-certified implementations were based on many types of enveloping methods: HTTP POST with name/value pairs, HTTP MIME Multipart, W3C XML Schema and SOAP+WSDL among others. Further, within each of these envelope method implementations, significant variations exist in field names and locations of Phase I Connectivity metadata, message envelope structure, authentication methods, routing approaches and security related information. Variations among enveloping methods and metadata pose a major challenge for interoperability.

The CORE Phase II Connectivity charge was to create a definitive Rule that would further facilitate interoperability. Such interoperability is expected to improve efficiencies and utilization of electronic transactions, and ultimately lower the administrative costs for healthcare providers and payers.

2.2 CORE Phase II Connectivity - Decisions on Message Envelope Standards

The CORE Phase II Connectivity efforts were focused on creating a definitive safe harbor that reached the envelope level. As part of CORE Phase II, the Connectivity & Security Subgroup performed extensive analysis of open standards that are available for enveloping the payload (ASC X12 or other types of data). The available open standards were rated against the agreed upon CORE Phase II Connectivity criteria and this rating process was used to select the envelope standards that met the large majority of these criteria; first creating a short-list and then reducing that short-list to two envelope standards that met the overwhelming majority of the criteria:

A. HTTP MIME Multipart

B. SOAP + WSDL

Over several months, discussions were held on the relative merits of these two envelope standards to determine if there is a clear winner among the two. SOAP+WSDL supports interface definition with a XSD schema/WSDL, automated development/validation, and is well aligned with standards adoption within healthcare industry bodies such as HL7 and HITSP. Furthermore, the SOAP+WSDL methodology lends itself to future Rule development using Web-Services standards for more advanced requirements like reliability. HTTP MIME Multipart on the other hand provides a relatively simple and well understood protocol framework and a lower performance overhead relative to SOAP, and has a large implementation base within this industry; including many of the CORE Phase I certified entities.

Having analyzed the advantages and challenges of the two envelope standards, CORE then analyzed several CORE Phase I Connectivity-compliant real world implementations of the above two envelope standards. The real world examples confirmed that both the envelope standards are in widespread use in this industry, and both perform well under real-world transaction volumes. Hence, the real-world implementation analysis did not point to a clear winner among the two envelope standards.

2.2.1 Why Two Standards in Phase II?

After extensive analysis, the two envelope standards (HTTP MIME Multipart and SOAP+WSDL) selected by the CORE Phase II Connectivity & Security Subgroup from the initial long list of standards were shown to:

- meet the CORE Phase II Connectivity criteria;
- have significant installed base in this industry; and,
- perform well under real world transaction loads.

Since both these standards have significant merits, the Subgroup debated the advantages and challenges of having a single envelope standard versus both these envelope standards as part of the CORE Phase II Rule and Safe Harbor. The major advantage of a Rule based on a single envelope standard is that it would be more definitive and facilitate better interoperability. However, having just one standard would require implementers of the other envelope standard (i.e., the one that was not chosen) to modify their implementations to be CORE Phase II-compliant. Since both standards met the criteria and have large installed bases, convergence on a single standard would create a barrier to adoption of CORE Phase II Connectivity Rule by a large segment of the industry. Moreover, the two standards have many similarities that the market is still exploring.

Based on the above analysis, the consensus view of the Subgroup was that a CORE Phase II Connectivity Rule should be based on both envelope standards. This provides CORE with a path to facilitate adoption in a market that is still maturing, and where many still require education. CORE recognizes that two standards do not support interoperability as much as one, however a CORE Phase II Rule and Safe Harbor based on two envelope standards would facilitate adoption while also improving interoperability relative to the current state of the industry. Given the current state of the industry, where the number of variations in the envelope standards and metadata is extremely large, reducing the number of envelope methods to two is a significant step forward in facilitating interoperability, improving efficiencies, improving utilization and hence lowering administrative cost for healthcare providers and health plans. Additionally, CORE is offering a path to use two standard market implementations – an option that does not exist today.

2.2.2 Will CORE Move to One Standard in Future Phases?

In the interest of further facilitating interoperability, CORE expects to move towards a single envelope standard in future phases. Given the current state of healthcare connectivity (i.e., use of many distinct connectivity methods), creating a CORE Phase II Connectivity rule with two envelope methods vastly improves the state of the market, while also providing an opportunity for education and greater experience with two standards that meet the growing market needs for connectivity. Taking this phased step enables the healthcare industry to make a more informed decision as it considers supporting a single envelope, safe harbor standard in future CORE phases.

The choice of two envelope standards provides this industry an opportunity to monitor the marketplace for movement towards a specific standard. Holding industry discussions on Phase II implementations will be essential to ensure that CORE continues to be aligned with the direction of related national healthcare initiatives.

2.3 Rationale for Basic Conformance Requirements

Supporting two envelope standards and two submitter authentication methods as part of the CORE Phase II Connectivity Rule makes it necessary to specify the conformance requirements for stakeholders. The rationale for these basic conformance requirements is based on the following guiding principles and assumptions.

It is assumed that the typical message exchange patterns are:

- *Real time*: Health plan receives a Real time request directly (or relayed via a Clearinghouse) from Providers and responds synchronously (as part of the same connection). A sequence diagram of the Real time Interaction is provided in Appendix 6.3.

- *Batch*: Health plan receives a Batch submission directly (or relayed via a Clearinghouse) from a Provider. Provider polls Health plan (directly or indirectly via a Clearinghouse) at a later time and receives an acknowledgement for the batch submission. Provider polls Health plan (directly or indirectly via a Clearinghouse) at a later time and retrieves the batch results as response. Provider then sends an acknowledgement to Health plan (directly or indirectly via a Clearinghouse) that the results were received with/without errors. A sequence diagram of the Batch Interaction is provided in Appendix 6.3.

In both of these message exchange patterns, Provider acts as a client, and Health Plan acts as a server, and Clearinghouse acts as both client and server.

One of the goals of CORE Connectivity is to improve utilization of electronic transactions by enabling more entities to interoperate with other entities, including reducing the implementation barrier for small entities (e.g., small providers).

Based on the above guiding principle and assumption about typical message exchange patterns, the rationale for the conformance requirements is as follows:

- Envelope standards: Organizations that receive and process or relay the requests (i.e., as a server) are required to support both envelope methods to facilitate connectivity from multiple clients. Generally organizations implementing a server have higher technical capabilities, and the difference in complexity between HTTP MIME Multipart and SOAP+WSDL are usually not significant for such organizations.
- Submitter authentication standards: Organizations that receive and process (or relay) requests (i.e., as a server) generally enforce a specific authentication method to control access to their resources. Supporting this authentication method is a credential issuance and management scheme defined by an organizational policy. The complexity of supporting two such policies and credential management mechanisms is high at the entity where submitter authentication is enforced (server), but is relatively low at the submitter (client). For this reason, server-side implementations are only required to support one of the two submitter authentication methods. To connect to the server, the client implementation needs to be able to authenticate itself to the server using the authentication method that is enforced at the server.

3 SCOPE

3.1 What the Rule Applies To

The technical scope of Phase II CORE Connectivity Rule can be described in terms of the specific network layers within the Open Systems Interconnection Basic Reference Model[1] (OSI model). As shown in the diagram below, the scope of Phase II CORE Connectivity Rule is OSI Layers 3 and 4 (Transport and Network layers) and OSI Layers 5 and 6 (Session and Presentation layers, also called Message Encapsulation layers). The Phase I CORE Connectivity Rule (i.e., *CORE Operating Rule 153: Connectivity Rule*) defined a Safe Harbor in terms of OSI Layers 3 and 4 (Transport and Network layers). CORE Phase II Connectivity Rule builds on the Phase I foundation and provides a more definitive Rule for encapsulating the metadata that is required for routing, identification/authentication and auditing.

[1] Zimmerman, H., OSI Reference Model – ISO Model of Architecture for Open Systems Interconnection, IEEE Transactions on Communications, Vol. Com-28, No. 4, April 1980.

Figure #3.3.1

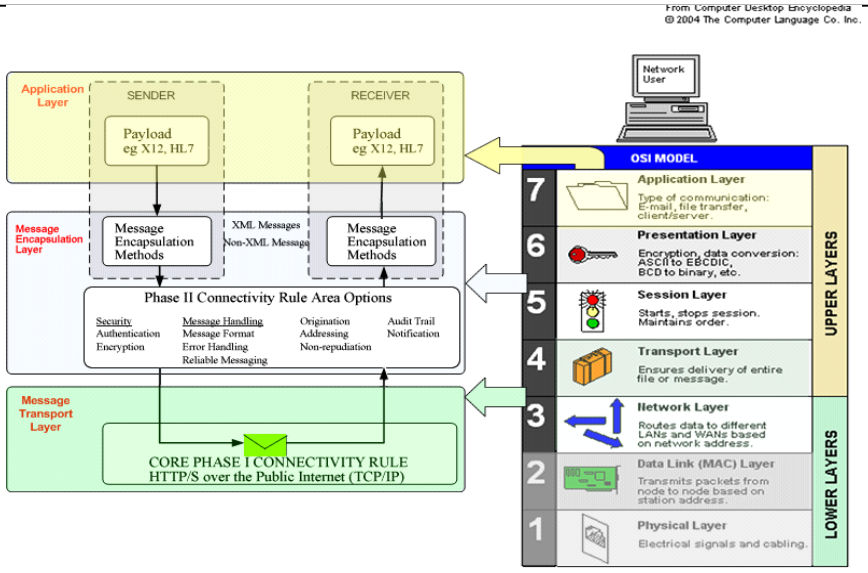


Figure Notes

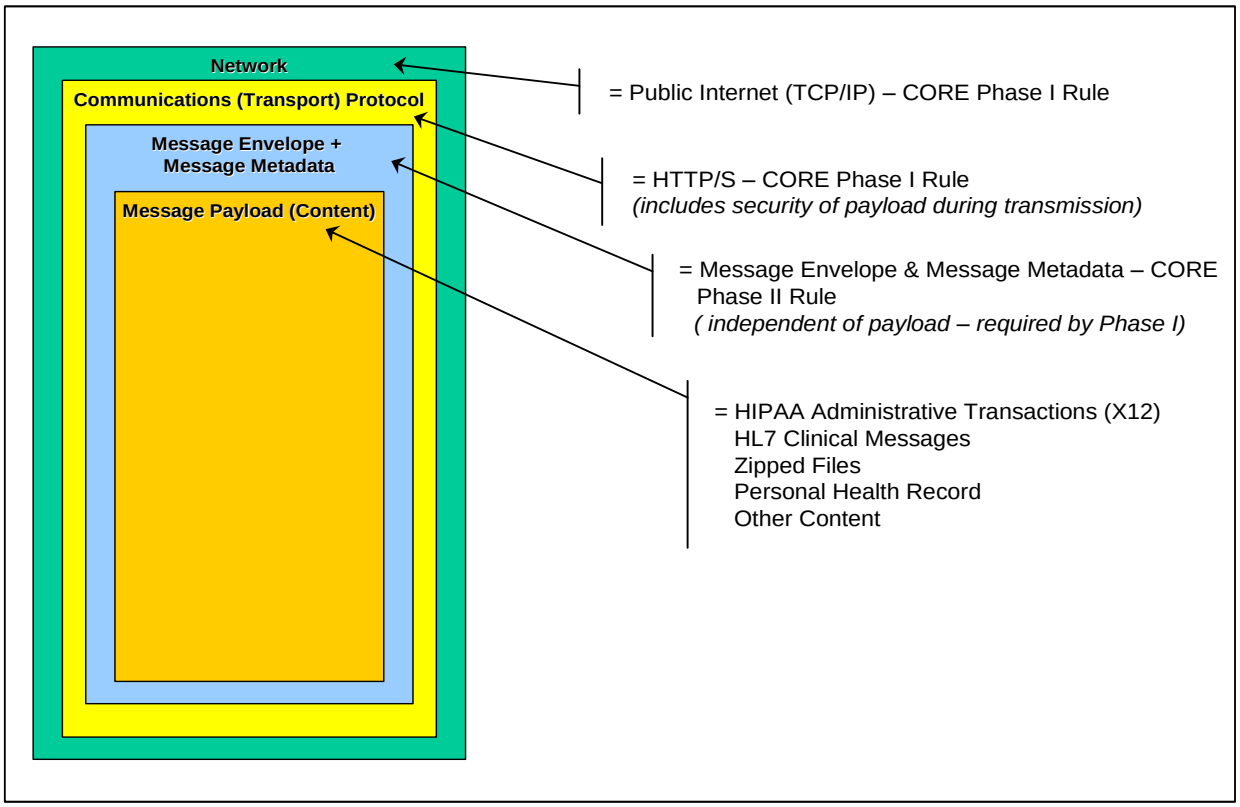
- Phase II Connectivity Rule addresses **Layers 5 and 6** of the OSI Model
- **Layer 3 and 4** the Transport Layer and Network Layer has already been designated as HTTP/S over the public internet in the Phase I Connectivity Rule
- **Layers 1 and 2** are not applicable to CORE because they are not items that could be included in a rule as these layers are so specific to the internal IT systems of every organization

OSI Model		Messaging Infrastructure Model	Addressed in
Application Layer	OSI7	Application Layer	Payload Standards (e.g., X12, HL7)
Presentation Layer	OSI6	Message Encapsulation Layer (envelope)	Phase II
Session Layer	OSI5		Phase II
Transport Layer	OSI4	Message Transport Layer	Phase I
Network Layer	OSI3		Phase I

As shown in the Figure 3.3.1 above, typically an application file (or Payload) such as X12 or HL7 is created or processed by an application that resides in the Application Layer (Layer 7 in the OSI Model). The Message Encapsulation layer (Layers 5 and 6 in the OSI Model) create a message envelope, and handle connectivity and security. The underlying layers (Layers 1 through 4) provide the necessary message transport and the network infrastructure (e.g., TCP/IP is provided at Layer 3).

As shown in Figure #3.3.2 below, the Message Envelope is outside the Message Payload (content), and inside the Transport Protocol envelope. Here, the Transport Protocol Envelope corresponds to OSI Model Layer 3 and 4, Message Envelope corresponds to OSI Model Layers 5 and 6, and Message Payload (content) corresponds to OSI Model Layer 7. The Phase I CORE 153 Connectivity Rule version 1.1.0 was based on the use of HTTP/S as the transport protocol over the public Internet; hence the transport protocol envelope consists of HTTP headers. Examples of message payload include HIPAA administrative transactions (ASC X12), HL7 clinical messages, zipped files, etc.

Figure #3.3.2



The following is a list of standards and their versions that this Rule is based on:

- HTTP Version 1.1
- SSL Version 3.0
    - This does not preclude the optional use of TLS 1.0 (or a higher version as required for FIPS 140 compliance) for connectivity with trading partners that require FIPS 140 compliance. CORE Connectivity certification requires testing with SSL 3.0 for transport security.
- MIME Version 1.0
- The MIME Multipart/Form-Data (IETF RFC 2388)
- SOAP Version 1.2
- WSDL Version 1.1
- Web Services-Security 1.1

3.2 When the Rule Applies

The Phase II CORE Connectivity Rule is applicable to Eligibility Benefit Inquiry and Response (270/271), Health Care Claim Status Request and Response (276/277), and Health Care Claim Acknowledgement (277) payloads in Real time and Batch mode, and may also be applied to other payload types. Note, some entities may also apply the rule to other ASC X12 administrative transactions. Phase II CORE Connectivity Rule is a Safe Harbor, and therefore only needs to be used if mutually agreed to by the trading partners. It is expected that in some instances, other or existing mechanisms may be more appropriate methods of Connectivity.

3.3 When the Rule Does Not Apply

The Phase II CORE Connectivity Rule **DOES NOT** apply in the following scenarios:

- When CORE-certified entities exchange payloads other than Eligibility, Claim Status and Claim Status-related payloads. This rule is designed to be payload agnostic, and as such it is expected that CORE-certified entities will use this methodology for payloads other than Eligibility, Claim Status and Claim Status-related payloads; however, the rule does not require this.
- When trading partners mutually agree to use a non-CORE connectivity mechanism.

3.4 What the Rule Does Not Require

The Phase II CORE Connectivity Rule:

- **DOES NOT** require trading partners to discontinue existing connections that do not match the rule.
- **DOES NOT** require that trading partners must use a CORE-complaint method for all new connections.
- **DOES NOT** require that all CORE trading partners use only one method for all connections.
- **DOES NOT** require any CORE-certified entity to do business with any trading partner or other CORE-certified entity.

Further, the Phase II CORE Connectivity Rule **DOES NOT** require the following:

- Additional centralized services other than those that are already provided in the Internet (e.g., Domain name and TCP/IP routing services).
- Additional directories or data repositories.
- Additional centralized Public Key Infrastructure (PKI) Certificate Authorities, identity management or authentication servers.
- Use of specific hardware platforms, software or programming languages.

3.5 Technical Requirements and Assumptions

The following technical requirement applies to this rule:

- The use of the public Internet for HTTP/S transport as specified in *Phase I CORE 153 Connectivity Rule.*

The following assumptions apply to this rule:

- Interoperability, utilization and efficiency will improve by having fewer connectivity/security variations and uniform enveloping standards and metadata.
- The typical message exchange patterns for Real time and Batch transactions are as described in §2.3.
- Health Plans and Clearinghouses generally have greater technical and infrastructure capabilities than most Providers.
- The difference in complexity between HTTP MIME Multipart and SOAP+WSDL is not significant for a server implementation.
- The Server-side enforcement of submitter authentication is far more complex than supporting the submitter authentication method on the client-side.
- This Rule is based upon a specific set of open standards and the versions of these standards specified in §3.1. As open standards and versions evolve, appropriate version control practices may need to be applied to keep the Rule consistent with industry best practices with regards to standard versions.
- This rule is a component of the larger set of Phase II CORE Rules; as such, all the CORE Guiding Principles apply to this rule and all other rules.

- All entities seeking Phase II certification will be Phase I certified, or concurrently testing for compliance with Phase I rules, as Phase I provides a foundation for Phase II CORE. The exception is vendors/clearinghouses that do not conduct the v5010 270/271 eligibility, or the 276/277 claim status, or the 277 claim acknowledgement transactions.

3.6 Outside the Scope of this Rule

The following items are outside the scope of this rule:

- The use of the message envelope and metadata defined in this rule for those messages that are sent over TCP/IP connections that are private (e.g., Intranet, leased lines, or VPN).
- Non-TCP/IP protocols such as packet switching (e.g., X.25, SNA, and Frame Relay).
- Application of this rule to other administrative transactions, such as 837 claims, as well as clinical or other transactions, e.g., HITSP interoperability specifications.
- Submitter Authorization is a local decision at the site that receives a request.
- The list of trusted Certificate Authorities is a decision between trading partners.
- The maximum size of a batch file that is accepted by a Server. The Server implementer may publish its file size limit, if any, in its Connectivity Companion Guide. (See §4.3.7)

3.7 Relationship to CORE Phase I Rule[2] and Safe Harbor

This Phase II Connectivity Rule extends the Phase I Connectivity Rule (i.e., *CORE Operating Rule 153: Connectivity Rule*) and establishes a Safe Harbor by further specifying the connectivity that all CORE-certified organizations must demonstrate and implement. See §5 CORE Safe Harbor. Each of the Phase I requirements has been incorporated in the Phase II Rule except that the HTTP error code for security authorization failures has been superseded under the SOAP option under this Rule. Under the Phase II SOAP option, security authorization failures will follow the SOAP standard.

Since the Phase II CORE Connectivity Safe Harbor and Rule is more definitive than the CORE Phase I Safe Harbor Connectivity Rule, those entities that achieve CORE Phase II Connectivity compliance are assumed to be CORE Phase I compliant, but such entities will not be required to support CORE Phase I connections. Should entities ask for CORE Phase I solutions rather than Phase II solutions, trading partners will mutually determine which option will be used.

Phase I Connectivity Rule elements re-used in this Phase II Rule:

- Transport standard (HTTP/S) (Phase I *CORE Operating Rule 153 Connectivity Rule*)
- Acknowledgements (Phase I *CORE Operating Rule 150 Batch Acknowledgements, CORE Operating Rule 151 Real Time Acknowledgements*)
- Response Time, Time Out, Re-transmission (Phase I *CORE Operating Rule 155 Batch Response Time Rule, CORE Operating Rule 156 Real Time Response Rule*)

Phase I Connectivity Rule (i.e., Phase I *CORE Operating Rule 153 Connectivity Rule*) elements modified in this Phase II Rule:

- Date/time syntax (to make it UTC standards compliant)

Phase I Connectivity Rule (i.e., Phase I *CORE Operating Rule 153 Connectivity Rule*) elements extended in this Phase II Rule:

- Envelope structure, metadata names and syntax
- Attachment handling

[2] Phase I CORE 153 Connectivity Rule.

- Authentication (e.g., *UserName* token for SOAP envelope)

4 RULE

This section specifies the basic conformance requirements, the envelope metadata and the specifications for HTTP MIME Multipart and SOAP+WSDL. The rationale and business justification for these conformance requirements are described in §2.3.

4.1 Basic Conformance Requirements for Key Stakeholders

Like the Phase I Connectivity Rule (CORE Operating Rule 153: Connectivity Rule), the Phase II Connectivity Rule is a Safe Harbor. CORE-certified entities are required to comply with all CORE Rules and thus a CORE-certified entity must support a CORE-compliant connectivity method. However, as a Safe Harbor the CORE Connectivity Rule:

- **DOES NOT** require trading partners to discontinue existing connections that do not match the rule.
- **DOES NOT** require that trading partners must use a CORE-complaint method for all new connections.
- **DOES NOT** require that all CORE trading partners use only one method for all connections.
- **DOES NOT** require any CORE-certified entity to do business with any trading partner or other CORE-certified entity.

The terms used in this Section, such as Client, Server, Envelope Standard A and B, Submitter Authentication Standard C and D, are defined in §6.1 *Abbreviations and Definitions used in this Rule*. The sections below specify the conformance requirements for stakeholders that can be CORE-certified, including Health Plans, Clearinghouses, Health Information Exchanges, and other intermediaries, Providers, Provider Vendors and Health Plan Vendors.

4.1.1 Health Plans and Health Plan Vendors

Health Plans or Health Plan Vendors (Servers) must implement capability to support (See §6.1) both Message Envelope Standards (A and B). For each envelope standard, the following are the conformance requirements for Real time and Batch transactions:

- Real time[3]: Required for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions
- Batch: Optional for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions; must be supported if Batch is offered for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions

Health Plans or Health Plan Vendors (Server) must implement and enforce one of the two (C or D) Submitter Authentication Standards for Phase II CORE Connectivity Compliance (for Real time and/or Batch transactions). If a Health Plan or Health Plan Vendor implements a client (e.g., for plan-to-plan messaging), then for such clients, the Health Plan or Health Plan Vendor must implement the capability to support one of the two Message Envelope Standards (A or B), and must implement support for both Submitter Authentication Standards (C and D).

4.1.2 Clearinghouses, Health Information Exchanges and Other Intermediaries

Intermediaries, including Clearinghouses, Switches, and Health Information Exchanges, act as both Client and Server. The Server portion of Clearinghouses/Switches/Health Information Exchanges must implement the capability to support both Message Envelope Standards (A and B). The Client portion of Clearinghouses/Switches/Health Information Exchanges must implement the capability to support one of the two Message Envelope Standards (A or B). For each envelope standard (A and B), the following are the conformance requirements for Real time and Batch transactions:

- Real time: Required for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions
- Batch: Optional for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions; must be supported if Batch is offered for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions

[3] Real time and Batch are defined in §6.1 Abbreviations and Definitions used in this Rule.

The Client portion of Clearinghouses/Switches/Health Information Exchanges must implement both (C and D) Submitter Authentication Standards for CORE Phase II Connectivity Compliance (for Real time and/or Batch transactions) to connect to Health Plans (i.e., as a client of the Health Plan). The Server portion of Clearinghouses/Switches/Health Information Exchanges must implement one of the two Authentication Standards for authenticating the Providers that submit requests to them (See Figure #4.1.6.1 for illustration).

If there is more than one intermediary (e.g., Clearinghouse/Switch/Health Information Exchange) between a Provider and Health Plan, then the Server portion of each intermediary must implement both Message Envelope Standards (A and B), and one of the two Submitter Authentication Standards (C or D). Further, the Client portion of each intermediary must implement one of the two Message Envelope Standards (A or B), and the Client portion must implement both the Submitter Authentication Standards (C and D).

4.1.3 Providers and Provider Vendors

Providers or Provider Vendors (Clients) must implement one of the two (A or B) Envelope Standards for Phase II CORE Connectivity Compliance. If a Provider or Provider Vendor implements a Server, then it must support both envelope methods (A and B) on the Server. For the Envelope Standard (A or B) implemented, the following are the conformance requirements for Real time and Batch transactions:

- Real time: Required for ASC X12 v5010 270/271 and ASC X12 2 v5010 76/277 transactions
- Batch: Optional for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions; must be supported if Batch is offered for ASC X12 v5010 270/271 and ASC X12 v5010 276/277 transactions

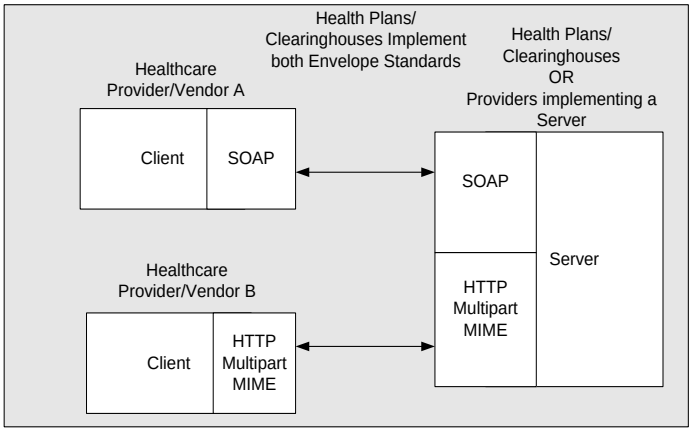
Providers or Provider Vendors must implement both (C and D) Submitter Authentication Standards for Phase II CORE Connectivity Compliance (for Real time and/or Batch transactions). If a Provider or Provider Vendor implements a Server, then it must support one of the two Submitter Authentication Standards on the Server.

4.1.4 Illustration of Conformance Requirements for Key Stakeholders

4.1.4.1 Envelope Standards

Figure #4.1.6.1 below shows the Phase II CORE Connectivity Rule's envelope standards conformance requirements for key stakeholders. Health Plans and Clearinghouses/Switches/Information Exchanges that conform to Phase II CORE Connectivity Rule must implement both envelope standards (SOAP+WSDL and HTTP MIME Multipart). Healthcare Providers or Provider Vendors must implement one of the envelope standards.

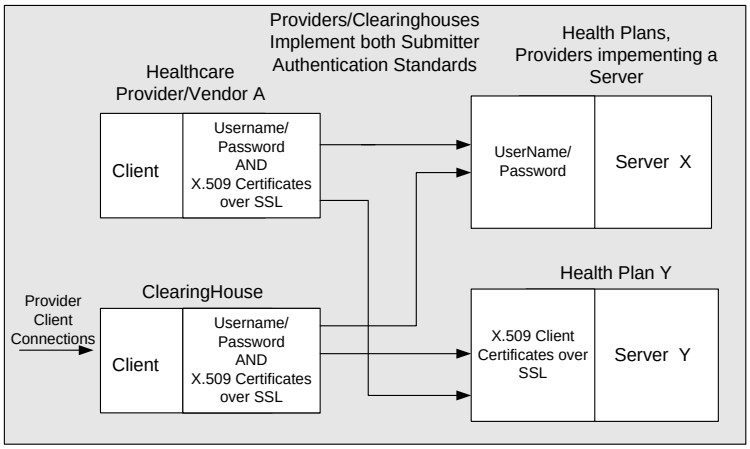
Figure #4.1.6.1



4.1.4.2 Submitter Authentication Standards

Figure #4.1.6.2 below shows the submitter authentication conformance requirements for key stakeholders. As shown, the Health Plans (servers) implement one of the two submitter Authentication Standards. Healthcare Providers/Provider Vendors and Clearinghouse components that handle submissions to Health Plans must implement both submitter Authentication Standards (i.e., only the client portion of authentication).

Figure #4.1.6.2



4.2 CORE-compliant Envelope Specifications using Message Enveloping Standards

CORE is not creating its own envelope standards, but rather, supports the use of existing standards. Note: The terms *normative* and *non-normative* are defined in *§6.1 Abbreviations and Definitions used in this Rule*.

4.2.1 Specifications for HTTP MIME Multipart (Envelope Standard A)

Unlike in the SOAP+WSDL (i.e., Envelope B) case, the HTTP MIME[4] Multipart envelope does not provide a standard Schema specification that is normative (definitive) and can be verified in an automated manner. For this reason, HTTP MIME Multipart Real time Request/Response examples below are non-normative[5]. They are based on the real-world examples provided by CORE participants, and have been updated to use the CORE-compliant metadata.

4.2.1.1 Real Time Request Message Structure (non-normative)

The following is an example of a Real time request message using the HTTP MIME Multipart envelope method. The HTTP Header is shown in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

e51d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"
```

[4] MIME Multipart is defined in IETF RFC 2388 (http://www.faqs.org/rfcs/rfc2388.html)
[5] The lack of a normative schema specification means that client-server interfaces need to be manually created and validated (i.e., automated interface generation and validation is not supported). This is not considered a significant limitation since the request/response interfaces are relatively simple to implement and validate.


```
hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"

<contents of file go here -- 1674 bytes long as specified above>
--XbCY--
```

4.2.1.2 Real Time Response Message Structure (non-normative)

The following is an example of a Real time response message using the HTTP MIME Multipart envelope method. The portion of the request below that is colored in blue is the HTTP Header. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_271_Response_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="ErrorCode"

Success
--XbCY
Content-Disposition: form-data; name="ErrorMessage"

None
--XbCY
Content-Disposition: form-data; name="Payload"

<contents of file go here -- 1674 bytes long as specified above>
--XbCY--
```


4.2.1.3 Batch Submission Message Structure (non-normative) [6]

The following is an example of a Batch Submission message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
POST /core/eligibility HTTP/1.1
Host: server host:server port
Content-Length: 244508
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Checksum"

6A3FE55946
--XbCY
Content-Disposition: form-data; name="Payload"

<contents of batch file go here>
--XbCY--
```

[6] Generic Batch Submission Request (§6.3.4) uses the same request message as the Batch Submission Request message structure above, with *PayloadType* values based on what is being submitted.

4.2.1.4 Batch Submission Response Message Structure (non-normative)[7]

The following is an example of a synchronous response to a Batch Submission request message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_BatchReceiptConfirmation
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="ErrorCode"

Success
--XbCY
Content-Disposition: form-data; name=”ErrorMessage”

None
--XbCY--
```

[7] Generic Batch Submission Response (§6.3.4) uses the same response message as the Batch Submission Response message structure depicted below, with *PayloadType* values based on the response to what is being submitted.

4.2.1.5 Batch Submission Acknowledgement Retrieval Request Message Structure (non-normative)

The following is an example of a Batch Submission Acknowledgement Retrieval request message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
POST /core/eligibility HTTP/1.1
Host: server host:server port
Content-Length: 244508
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_999_RetrievalRequest_005010X231A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY--
```


4.2.1.6 Batch Submission Acknowledgement Retrieval Response Message Structure (non-normative)

The following is an example of a Batch Submission Acknowledgement Retrieval Response message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 12648
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_999_Response_005010X231A1[8]
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Checksum"

6A3FE55946
--XbCY
Content-Disposition: form-data; name="Payload"

<contents of batch file go here>
--XbCY
Content-Disposition: form-data; name="ErrorCode"

Success
--XbCY
Content-Disposition: form-data; name="ErrorMessage"

None
--XbCY--
```

[8] Although this example shows a 999 payload type being sent as a response from a server to the client, this could also include a TA1. Alternatively, the server may elect to send only a TA1 without any functional group.

4.2.1.7 Batch Results Retrieval Request Message Structure (non-normative)[9]

The following is an example of a Batch Results Retrieval request message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
POST /core/eligibility HTTP/1.1
Host: server host:server port
Content-Length: 244508
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_005010_Request_Batch_Results_271
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY--
```

[9] Generic Batch Retrieval Request (§6.3.3) uses the same request message as the Batch Results Retrieval Request message structure depicted below, with different *PayloadType* values based on what is being retrieved.

4.2.1.8 Batch Results Retrieval Response Message Structure (non-normative) [10]

The following is an example of a Batch Retrieval Response message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 12648
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_271_Response_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
None
--XbCY
Content-Disposition: form-data; name="Checksum"

6A3FE55946
--XbCY
Content-Disposition: form-data; name="Payload"
<contents of batch file go here>
--XbCY
Content-Disposition: form-data; name="ErrorCode"

Success
--XbCY
Content-Disposition: form-data; name="ErrorMessage"

None
--XbCY--
```

[10] Generic Batch Retrieval Response (§6.3.3) uses the same response message as the Batch Results Retrieval Response message structure depicted below, with different *PayloadType* values based on the response to what is being retrieved.

4.2.1.9 Batch Results Acknowledgement Submission Message Structure (non-normative)[11]

The following is an example of a Batch Results Acknowledgement Submission message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
POST /core/eligibility HTTP/1.1
Host: server host:server port
Content-Length: 244508
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12 999 SubmissionRequest 005010X231A1[12]
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Checksum"

6A3FE55946
--XbCY
Content-Disposition: form-data; name="Payload"

<contents of batch file go here>
--XbCY--
```

[11] Generic Batch Receipt Confirmation (§6.3.3) uses the same request message as the Batch Results Acknowledgement Submission message structure depicted below, with different *PayloadType* values as appropriate.
[12] Although this example shows a 999 payload type being submitted by the client to the server, this could also include a TA1. Alternatively, the client may elect to submit only a TA1 without any functional group.

4.2.1.10 Batch Results Acknowledgement Submission Response Message Structure (non-normative) [13]

The following is an example of a Batch Results Acknowledgement Submission Response message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_Response_ConfirmReceiptReceived
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="ErrorCode"

Success
--XbCY
Content-Disposition: form-data; name=”ErrorMessage”

None
--XbCY--
```

[13] Generic Batch Receipt Confirmation Response (§6.3.3) uses the same request message as the Batch Results Acknowledgement Submission Response message structure depicted below, with different *PayloadType* values as appropriate.

4.2.1.11 Envelope Processing Error Message Structure (non-normative)

The following is an example of an Envelope Processing Error message using the HTTP MIME Multipart envelope method. The HTTP Headers are shown colored in blue. The remainder of the request (shaded in light gray) is the body of the MIME Multipart message.

```
HTTP/1.1 200 OK
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

COREEnvelopeError
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0a91e6fa6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"

PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="ErrorCode"

VersionMismatch
--XbCY
Content-Disposition: form-data; name=”ErrorMessage”

Expected Version X, received version Y
--XbCY—
```

4.2.1.12 Payload Attachment Handling

The Payload must be sent as a MIME Multipart attachment for both Real time as well as Batch transactions.

4.2.2 Specifications for SOAP+WSDL (normative[14]) (Envelope Standard B)

This section defines the SOAP+WSDL envelope method for CORE Phase II Connectivity. The XML Schema that is defined below is used within the Web Services Definition Language (WSDL) specification.

Note: The terms SOAP, WSDL, MTOM, Normative and Non-normative are defined in *Appendix §6.1: Abbreviations and Definitions used in this Rule*.

[14] See §6.1 Abbreviations and Definitions used in this Rule for a definition of Normative.

4.2.2.1 CORE Phase II Connectivity XML Schema Specification (normative)

The CORE Phase II compliant XML Schema Specification file name below is called *CORERule2.2.0.xsd*, and is available at http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd. This schema has ten elements, each representing a type of request or response message envelope:

- Real time Request Schema (Element name is *COREEnvelopeRealTimeRequest*)
- Real time Response (Element name is *COREEnvelopeRealTimeResponse*)
- Batch Submission (Element name is *COREEnvelopeBatchSubmission*)
- Batch Submission Response (Element name is *COREEnvelopeBatchSubmissionResponse*)
- Batch Submission Acknowledgement Retrieval Request (Element name is *COREEnvelopeBatchSubmissionAckRetrievalRequest*)
- Batch Submission Acknowledgement Retrieval Response (Element name is *COREEnvelopeBatchSubmissionAckRetrievalResponse*)
- Batch Results Retrieval Request (Element name is *COREEnvelopeBatchResultsRetrievalRequest*)
- Batch Results Retrieval Response (Element name is *COREEnvelopeBatchResultsRetrievalResponse*)
- Batch Results Acknowledgement Submission (Element name is *COREEnvelopeBatchResultsAckSubmission*)
- Batch Results Acknowledgement Submission Response (Element name is *COREEnvelopeBatchResultsAckSubmission Response*)


```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd"
targetNamespace="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <xs:element name="COREEnvelopeRealTimeRequest">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="Payload" type="xs:string" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="COREEnvelopeRealTimeResponse">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="Payload" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="COREEnvelopeBatchSubmission">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadLength" type="xs:int" minOccurs="1" maxOccurs="1"/>
        <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CheckSum" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="Payload" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="COREEnvelopeBatchSubmissionResponse">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
        <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="COREEnvelopeBatchSubmissionAckRetrievalRequest">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
```



```
      <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="COREEnvelopeBatchSubmissionAckRetrievalResponse">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
      <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
      <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="COREEnvelopeBatchResultsRetrievalRequest">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
      <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="COREEnvelopeBatchResultsRetrievalResponse">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
      <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
      <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="COREEnvelopeBatchResultsAckSubmission">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
      <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
```



```
    </xs:complexType>
  </xs:element>
  <xs:element name="COREEnvelopeBatchResultsAckSubmissionResponse">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
        <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ErrorCode" type="xs:string"  minOccurs="1" maxOccurs="1"/>
        <xs:element name="ErrorMessage" type="xs:string"  minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:simpleType name="RealTimeMode">
    <xs:restriction base="xs:string">
      <xs:pattern value="RealTime"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="BatchMode">
    <xs:restriction base="xs:string">
      <xs:pattern value="Batch"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

4.2.2.2 CORE Phase II Connectivity Web Services Definition Language (WSDL) Specification (normative)

The CORE Phase II Connectivity Web Services Definition Language (WSDL) file below is called *CORERule2.2.0.wsdl*, and is available at *www.caqh.org/SOAP/WSDL/CORERule2.2.0.wsdl*. The WSDL below makes use of the XML Schema (CORERule2.2.0.xsd) as specified in §4.2.2.1. Within this WSDL the following types of messages are defined:

- Real time Request Message (Message name is *RealTimeRequestMessage*)
- Real time Response Message (Message name is *RealTimeResponseMessage*)
- Batch Submission Request Message (Message name is *BatchSubmissionMessage*)
- Batch Submission Response Message (Message name is *BatchSubmissionResponseMessage*)
- Batch Submission Acknowledgement Retrieval Request (Message name is *BatchSubmissionAckRetrievalRequestMessage*)
- Batch Submission Acknowledgement Retrieval Response (Message name is *BatchSubmissionAckRetrievalResponseMessage*)
- Batch Results Retrieval Request Message (Message name is *BatchResultsRetrievalRequestMessage*)
- Batch Results Retrieval Response Message (Message name is *BatchResultsRetrievalResponseMessage*)
- Batch Results Acknowledgement Submission Message (Message name is *BatchResultsAckSubmissionMessage*)
- Batch Results Acknowledgement Submission Response Message (Message name is *BatchResultsAckSubmissionResponseMessage*)

Using the above message definitions, the following types of transactions are defined:

- Real time Transaction (Operation name is *RealTimeTransaction*)
- Batch Submit Transaction (Operation name is *BatchSubmitTransaction*)
- Batch Submit Acknowledgement Retrieval Transaction (Operation name is *BatchSubmitAckRetrievalTransaction*)
- Batch Results Retrieval Transaction (Operation name is *BatchResultsRetrievalTransaction*)

- Batch Results Acknowledgement Transaction (Operation name is *BatchResultsAckSubmitTransaction*)
- Generic Batch Retrieval Transaction (Operation name is *GenericBatchRetrievalTransaction)*
- Generic Batch Receipt Confirmation Transaction (Operation name is *GenericBatchReceiptConfirmationTransaction)*
- Generic Batch Submission Transaction (Operation name is *GenericBatchSubmissionTransaction*)

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:CORE="http://www.caqh.org/SOAP/WSDL/"
                              xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
                              xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                              xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                              xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                              xmlns:CORE-XSD="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd"
                              xmlns="http://schemas.xmlsoap.org/wsdl/"
                              name="CORE"
                              targetNamespace="http://www.caqh.org/SOAP/WSDL/">
  <wsdl:types>
    <xsd:schema xmlns="http://schemas.xmlsoap.org/wsdl/"
                                          elementFormDefault="qualified"
                                          targetNamespace="http://www.caqh.org/SOAP/WSDL/">
      <xsd:import namespace="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd"
schemaLocation="CORERule2.2.0.xsd"/>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="RealTimeRequestMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeRealTimeRequest"/>
  </wsdl:message>
  <wsdl:message name="RealTimeResponseMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeRealTimeResponse"/>
  </wsdl:message>
  <wsdl:message name="BatchSubmissionMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchSubmission"/>
  </wsdl:message>
  <wsdl:message name="BatchSubmissionResponseMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchSubmissionResponse"/>
  </wsdl:message>
  <wsdl:message name="BatchSubmissionAckRetrievalRequestMessage">
    <wsdl:part name="body"
                element="CORE-XSD:COREEnvelopeBatchSubmissionAckRetrievalRequest"/>
  </wsdl:message>
  <wsdl:message name="BatchSubmissionAckRetrievalResponseMessage">
    <wsdl:part name="body"
              element="CORE-XSD:COREEnvelopeBatchSubmissionAckRetrievalResponse"/>
  </wsdl:message>
  <wsdl:message name="BatchResultsRetrievalRequestMessage">
    <wsdl:part name="body"
                  element="CORE-XSD:COREEnvelopeBatchResultsRetrievalRequest"/>
  </wsdl:message>
  <wsdl:message name="BatchResultsRetrievalResponseMessage">
    <wsdl:part name="body"
                  element="CORE-XSD:COREEnvelopeBatchResultsRetrievalResponse"/>
  </wsdl:message>
  <wsdl:message name="BatchResultsAckSubmissionMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchResultsAckSubmission"/>
  </wsdl:message>
  <wsdl:message name="BatchResultsAckSubmissionResponseMessage">
    <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchResultsAckSubmissionResponse"/>
 </wsdl:message>
  <wsdl:portType name="CORETransactions">
    <wsdl:operation name="RealTimeTransaction">
      <wsdl:input message="CORE:RealTimeRequestMessage"/>
      <wsdl:output message="CORE:RealTimeResponseMessage"/>
    </wsdl:operation>
    <wsdl:operation name="BatchSubmitTransaction">
      <wsdl:input message="CORE:BatchSubmissionMessage"/>
      <wsdl:output message="CORE:BatchSubmissionResponseMessage"/>
    </wsdl:operation>
   <wsdl:operation name="GenericBatchSubmissionTransaction">
      <wsdl:input message="CORE:BatchSubmissionMessage"/>
      <wsdl:output message="CORE:BatchSubmissionResponseMessage"/>
    </wsdl:operation>
```



```
    <wsdl:operation name="BatchSubmitAckRetrievalTransaction">
      <wsdl:input message="CORE:BatchSubmissionAckRetrievalRequestMessage"/>
      <wsdl:output message="CORE:BatchSubmissionAckRetrievalResponseMessage"/>
    </wsdl:operation>
    <wsdl:operation name="BatchResultsRetrievalTransaction">
      <wsdl:input message="CORE:BatchResultsRetrievalRequestMessage"/>
      <wsdl:output message="CORE:BatchResultsRetrievalResponseMessage"/>
    </wsdl:operation>
    <wsdl:operation name="BatchResultsAckSubmitTransaction">
      <wsdl:input message="CORE:BatchResultsAckSubmissionMessage"/>
      <wsdl:output message="CORE:BatchResultsAckSubmissionResponseMessage"/>
    </wsdl:operation>
<wsdl:operation name="GenericBatchRetrievalTransaction">
      <wsdl:input message="CORE:BatchResultsRetrievalRequestMessage"/>
      <wsdl:output message="CORE:BatchResultsRetrievalResponseMessage"/>
    </wsdl:operation>
    <wsdl:operation name="GenericBatchReceiptConfirmationTransaction">
      <wsdl:input message="CORE:BatchResultsAckSubmissionMessage"/>
      <wsdl:output message="CORE:BatchResultsAckSubmissionResponseMessage"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="CoreSoapBinding" type="CORE:CORETransactions">
    <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="RealTimeTransaction">
      <soap12:operation soapAction="RealTimeTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="BatchSubmitTransaction">
      <soap12:operation soapAction="BatchSubmitTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
<wsdl:operation name="GenericBatchSubmissionTransaction">
      <soap12:operation
                          soapAction="GenericBatchSubmissionTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="BatchSubmitAckRetrievalTransaction">
      <soap12:operation
                          soapAction="BatchSubmitAckRetrievalTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="BatchResultsRetrievalTransaction">
      <soap12:operation
                          soapAction="BatchResultsRetrievalTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="BatchResultsAckSubmitTransaction">
      <soap12:operation
                            soapAction="BatchResultsAckSubmitTransaction" style="document"/>
      <wsdl:input>
```



```
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="GenericBatchRetrievalTransaction">
      <soap12:operation
                          soapAction="GenericBatchRetrievalTransaction" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
     <wsdl:operation name="GenericBatchReceiptConfirmationTransaction">
      <soap12:operation
                            soapAction="GenericBatchReceiptConfirmationTransaction"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="Core">
    <wsdl:port name="CoreSoapPort" binding="CORE:CoreSoapBinding">
      <soap12:address location="http://URL OF WEB SERVICE"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

The following sections show Request and Response messages using the SOAP envelope, based on the WSDL schemas defined above. The SOAP Real time Request/Response examples below are non-normative[15]. They are based on the real-world examples provided by CORE participants, but have been updated to use the CORE-recommended metadata that is part of CORE Phase II Connectivity.

4.2.2.3 Real Time Request Message Structure (non-normative)

The Real time Request message structure shown below specifies SOAP 1.2.

SOAP version 1.2 must be implemented by all Servers.

When sending or receiving payloads which contain non-printable characters, e.g., separator characters in an ASC X12 Interchange payload or in a non-ASC X12 Interchange payload in Real time using SOAP, the payload must be Base64 encoded.

This shows the following components:

1. The HTTP Headers are shown colored in blue.
2. The WS-Security Username and Password token (shown here with a pink background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.
3. The portion of the SOAP envelope colored in green has the remaining metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

[15] A non-normative description is informational only. See §6.1 Abbreviations and Definitions Used in this Rule.


```
POST /core/eligibility HTTP/1.1
Host: server host:server port
Content-Type: application/soap+xml; charset=UTF-8; action="RealTimeTransaction"

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Header>
       <wsse:Security
       xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
       1.0.xsd" soapenv:mustUnderstand="true">
       <wsse:UsernameToken xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
       wssecurity-utility-1.0.xsd wsu:Id="UsernameToken-21621663">
       <wsse:Username>bob</wsse:Username>
       <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
       token-profile-1.0#PasswordText">bobPW</wsse:Password>
       </wsse:UsernameToken>
       </wsse:Security>
       </soapenv:Header>
        <soapenv:Body>
              <ns1:COREEnvelopeRealTimeRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                <PayloadType> X12_270_Request_005010X279A1</PayloadType>
                      <ProcessingMode>RealTime</ProcessingMode>
                      <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>HospitalA</SenderID>
                      <ReceiverID>PayerB</ReceiverID>
                      <CORERuleVersion>2.2.0</CORERuleVersion>
         <Payload><![CDATA[ISA*00* *00* *ZZ*NEHEN780 *ZZ*NEHEN003 ...IEA*1*000000031]]></Payload>
              </ns1:COREEnvelopeRealTimeRequest>
                </soapenv:Body>
</soapenv:Envelope>
```

4.2.2.4 Real Time Response Message Structure (non-normative)

The Real time Response message structure shown below specifies SOAP 1.2. The HTTP Header is shown in blue. The remainder of the request is the SOAP Envelope. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml;
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransactionResponse";charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeRealTimeResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0xsd">
                      <PayloadType>X12_271_Response_005010X279A1</PayloadType>
                      <ProcessingMode>RealTime</ProcessingMode>
                      <PayloadID>a81d44ae-7dec-11d0-a765-00a0c91e6ba0</PayloadID>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>PayerB</SenderID>
                      <ReceiverID>HospitalA</ReceiverID>
                      <CORERuleVersion>2.2.0</CORERuleVersion>
           <Payload><![CDATA[ISA*00* *00* *ZZ*NEHEN780 *ZZ*NEHEN003
...IEA*1*000000031]]></Payload>
                      <ErrorCode>Success</ErrorCode>
                      <ErrorMessage></ErrorMessage>
                </ns1:COREEnvelopeRealTimeResponse>
         </soapenv:Body>
  </soapenv:Envelope>
```

4.2.2.5 Batch Submission Message (non-normative) [16]

The Batch Submission message structure shown below specifies SOAP 1.2, and also uses MTOM (See §6.1) to send the payload file. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The WS-Security Username and Password token (shown here with a pink background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.
3. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)
4. The Batch file (MTOM attachment) is shown colored in orange.

```
POST /core/eligibilityBatch HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org"; start-
info="application/soap+xml"; action="BatchSubmitTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Header>
       <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
       secext-1.0.xsd" soapenv:mustUnderstand="true">
       <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
       wssecurity-utility-1.0.xsd" wsu:Id="UsernameToken-21621664">
       <wsse:Username>bob</wsse:Username>
       <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
       profile-1.0#PasswordText">bobPW</wsse:Password>
       </wsse:UsernameToken>
       </wsse:Security>
       </soapenv:Header>
       <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmission
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                     <PayloadType>X12 270 Request 005010X279A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <PayloadLength>1551254</PayloadLength>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>2.2.0</CORERuleVersion>
                     <CheckSum>43B8485AB5</CheckSum>
                   <Payload>
                   <xop:Include      href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                   xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                     </Payload>
              </ns1:COREEnvelopeBatchSubmission>
        </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<Mixed batch file>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

[16] The Generic Batch Submission Request (§6.3.4) uses the same request message as the Batch Submission Request message structure depicted below, with *PayloadType* values based on what is being submitted.

4.2.2.6 Batch Submission Response Message (non-normative)[17]

The Batch Submission Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/BatchSubmitTransactionResponse"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                        <PayloadType>X12_BatchReceiptConfirmation</PayloadType>
                        <ProcessingMode>Batch</ProcessingMode>
                        <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                        <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                        <SenderID>PayerB</SenderID>
                        <ReceiverID>HospitalA</ReceiverID>
                        <CORERuleVersion>2.2.0</CORERuleVersion>
                        <ErrorCode>Success</ErrorCode>
                        <ErrorMessage></ErrorMessage>
                 </ns1:COREEnvelopeBatchSubmissionResponse>
         </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

4.2.2.7 Batch Submission Acknowledgement Retrieval Request Message (non-normative)

The Batch Submission Acknowledgement Retrieval Request message structure shown below specifies SOAP 1.2. The use of MTOM in Batch mode request/response creates multipart MIME even though there is no payload. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The WS-Security Username and Password token (shown here with a pink background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.
3. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

[17] The Generic Batch Submission Response (§6.3.4) uses the same response message as the Batch Submission Response message structure depicted below, with *PayloadType* values based on the response to what is being submitted.


```
POST /core/eligibilityBatch HTTP/1.1
Content-Type:      multipart/related;      boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml";     start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org";     start-
info="application/soap+xml"; action="BatchSubmitAckRetrievalTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Header>
       <wsse:Security     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
       secext-1.0.xsd"                                                    soapenv:mustUnderstand="true">
       <wsse:UsernameToken           xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
       wssecurity-utility-1.0.xsd"                                    wsu:Id="UsernameToken-21621664">
       <wsse:Username>bob</wsse:Username>
       <wsse:Password       Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
       profile-1.0#PasswordText">bobPW</wsse:Password>
       </wsse:UsernameToken>
       </wsse:Security>
       </soapenv:Header>
       <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionAckRetrievalRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                     <PayloadType>X12 999 RetrievalRequest 005010X231A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>2.2.0</CORERuleVersion>
                </ns1:COREEnvelopeBatchSubmissionAckRetrievalRequest>
         </soapenv:Body>
  </soapenv:Envelope>
--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

4.2.2.8 Batch Submission Acknowledgement Retrieval Response Message (non-normative)[18]

The Batch Submission Acknowledgement Retrieval Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)
3. The MTOM Attachment is colored in orange.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:       multipart/related;       boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml";      start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org";      start-
info="application/soap+xml"; action="BatchSubmitAckRetrievalTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionAckRetrievalResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                    <PayloadType>X12_999_Response_005010X231A1</PayloadType>
                    <ProcessingMode>Batch</ProcessingMode>
                    <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                    <PayloadLength>1551254</PayloadLength>
                    <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                    <SenderID>PayerB</SenderID>
                    <ReceiverID>HospitalA</ReceiverID>
                    <CORERuleVersion>~~2.0.1~~2.2.0</CORERuleVersion>
                    <CheckSum>43B8485AB5</CheckSum>
                   <Payload>
                  <xop:Include        href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                  xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                    </Payload>
                    <ErrorCode>Success</ErrorCode>
                    <ErrorMessage></ErrorMessage>
              </ns1:COREEnvelopeBatchSubmissionAckRetrievalResponse>
         </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<999 file>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

4.2.2.9 Batch Results Retrieval Request Message (non-normative) [19]

The Batch Results Retrieval Request message structure shown below specifies SOAP 1.2. The use of MTOM in Batch mode request/response creates multipart MIME even though there is no payload (which may be the case for a Batch Retrieval Request). This shows the following:

1. The HTTP Headers are shown colored in blue.

[18] Although this example shows a 999 payload type being sent as a response from a server to the client, this could also include a TA1. Alternatively, the server may elect to send only a TA1 without any functional group.

[19] The Generic Batch Retrieval Request (§6.3.3) uses the same request message as the Batch Results Retrieval Request message structure depicted below, with different *PayloadType* values based on what is being retrieved.

2. The WS-Security Username and Password token (shown here with a pink background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.

3. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

```
POST /core/eligibilityBatch HTTP/1.1
Content-Type:      multipart/related;      boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml";     start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org";     start-
info="application/soap+xml"; action="BatchResultsRetrievalTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Header>
       <wsse:Security     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
       secext-1.0.xsd"                                                    soapenv:mustUnderstand="true">
       <wsse:UsernameToken           xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
       wssecurity-utility-1.0.xsd"                                    wsu:Id="UsernameToken-21621664">
       <wsse:Username>bob</wsse:Username>
       <wsse:Password      Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
       profile-1.0#PasswordText">bobPW</wsse:Password>
       </wsse:UsernameToken>
       </wsse:Security>
       </soapenv:Header>
       <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsRetrievalRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
               <PayloadType>X12 005010 Request Batch Results 271</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>2.2.0</CORERuleVersion>
              </ns1:COREEnvelopeBatchResultsRetrievalRequest>
        </soapenv:Body>
  </soapenv:Envelope>
--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

4.2.2.10 Batch Results Retrieval Response Message (non-normative) [20]

The Batch Results Retrieval Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)
3. The MTOM Attachment is colored in orange.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:      multipart/related;      boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml";     start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org";     start-
info="application/soap+xml"; action="BatchResultsRetrievalTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsRetrievalResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                        <PayloadType>X12_271_Response_005010X279A1</PayloadType>
                        <ProcessingMode>Batch</ProcessingMode>
                        <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                        <PayloadLength>1551254</PayloadLength>
                        <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                        <SenderID>PayerB</SenderID>
                        <ReceiverID>HospitalA</ReceiverID>
                        <CORERuleVersion>2.2.0</CORERuleVersion>
                        <CheckSum>43B8485AB5</CheckSum>
                      <Payload>
                      <xop:Include       href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                      xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                        </Payload>
                        <ErrorCode>Success</ErrorCode>
                        <ErrorMessage></ErrorMessage>
                 </ns1:COREEnvelopeBatchResultsRetrievalResponse>
         </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<Response batch file>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

4.2.2.11 Batch Results Acknowledgement Submission Message (non-normative) [21]

The Batch Results Acknowledgement Submission message structure shown below specifies SOAP 1.2, and also uses MTOM (See §6.1) to send the payload file. This shows the following:

1. The HTTP Headers are shown colored in blue.

[20] The Generic Batch Retrieval Response (§6.3.3) uses the same response message as the Batch Results Retrieval Response message structure depicted below, with different *PayloadType* values based on the response to what is being retrieved.
[21] The Generic Batch Receipt Confirmation (§6.3.3) uses the same request message as the Batch Results Acknowledgement Submission message structure depicted below, with different *PayloadType* values as appropriate.

2. The WS-Security Username and Password token (shown here with a pink background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.

3. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

4. The Batch file (MTOM attachment) is shown colored in orange.

```
POST /core/eligibilityBatch HTTP/1.1
Content-Type:      multipart/related;      boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml";     start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org";     start-
info="application/soap+xml"; action="BatchResultsAckTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Header>
       <wsse:Security     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
       secext-1.0.xsd"                                                    soapenv:mustUnderstand="true">
       <wsse:UsernameToken           xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
       wssecurity-utility-1.0.xsd"                                      wsu:Id="UsernameToken-21621664">
       <wsse:Username>bob</wsse:Username>
       <wsse:Password       Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
       profile-1.0#PasswordText">bobPW</wsse:Password>
       </wsse:UsernameToken>
       </wsse:Security>
       </soapenv:Header>
       <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsAckSubmission
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                     <PayloadType>X12_999_SubmissionRequest_005010X231A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <PayloadLength>1551254</PayloadLength>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>2.2.0</CORERuleVersion>
                     <CheckSum>43B8485AB5</CheckSum>
                   <Payload>
                   <xop:Include       href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                   xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                     </Payload>
              </ns1:COREEnvelopeBatchResultsAckSubmission>
        </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<999 file>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

4.2.2.12 Batch Results Acknowledgement Submission Response Message (non-normative)[22]

The Batch Results Acknowledgement Submission Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

[22] The Generic Batch Receipt Confirmation Response (§6.3.3) uses the same response message as the Batch Results Acknowledgement Submission Response message structure depicted below, with different *PayloadType* values as appropriate.

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the CORE Phase II Connectivity Rule. (See §4.4)

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:  multipart/related;  boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml"; action="BatchResultsAckTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsAckSubmissionResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                    <PayloadType>X12_Response_ConfirmReceiptReceived</PayloadType>
                      <ProcessingMode>Batch</ProcessingMode>
                      <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>PayerB</SenderID>
                      <ReceiverID>HospitalA</ReceiverID>
                      <CORERuleVersion>2.2.0</CORERuleVersion>
                      <ErrorCode>Success</ErrorCode>
                      <ErrorMessage></ErrorMessage>
                </ns1:COREEnvelopeBatchResultsAckSubmissionResponse>
         </soapenv:Body>
  </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

4.2.2.13 ErrorMessage Structure (non-normative)

The Error message structure shown below uses the SOAP Fault specifications within SOAP 1.2. As described in §4.3.3: Error Handling, SOAP Faults must be used to send errors at the SOAP level. The HTTP Headers are shown colored in blue. The remainder of the request is the SOAP Envelope.

```
HTTP/1.1 500
Content-Length: 2408
Content-Type: application/soap+xml


<soapenv:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns: soapenv ="
http://www.w3.org/2003/05/soap-envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Header>

</soapenv:Header>

<soapenv:Body>

  <soapenv:Fault>
   <soapenv:Code><env:Value>env:Client</env:Value></env:Code>
    <soapenv:Reason>
      <soapenv:Text xml:lang="en">There was an error in the incoming SOAP request</env:Text>
    </soapenv:Reason>
   </soapenv:Fault>
</soapenv:Body>

</soapenv:Envelope>
```

4.2.2.14 Envelope Processing Error Message (non-normative)

The Error message structure shown below uses the SOAP Fault specifications within SOAP 1.2. The HTTP Headers are shown colored in blue. The remainder of the request is the SOAP Envelope. The envelope structure and metadata that is defined within CORE Phase II Connectivity Rule is colored in green.


```
HTTP/1.1 200 OK
Content-Type: application/soap+xml;
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransactionResponse";charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeRealTimeResponse xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                     <PayloadType>CoreEnvelopeError</PayloadType>
                     <ProcessingMode>RealTime</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>PayerB</SenderID>
                     <ReceiverID>HospitalA</ReceiverID>
                     <CORERuleVersion>2.2.0</CORERuleVersion>
                     <Payload></Payload>
                     <ErrorCode>VersionMismatch</ErrorCode>
                     <ErrorMessage>Expecting Version X, received Version Y</ErrorMessage>
              </ns1:COREEnvelopeRealTimeResponse>
         </soapenv:Body>
  </soapenv:Envelope>
```

4.2.2.15 Payload Attachment Handling

Real Time

- Payload must be embedded using the Inline method (using CDATA element as shown above).

Batch

- Payload must be sent as an MTOM[23] encapsulated MIME part.

4.3 General Specifications Applicable to Both Envelope Methods

The following sections specify requirements of the CORE Phase II Connectivity Rule that are applicable to both envelope methods (HTTP MIME Multipart and SOAP+WSDL).

4.3.1 Request and Response Handling

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 ASC 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.

4.3.1.1 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 §4.3.3 Error Handling) or the corresponding ASC X12 message response (e.g., a TA1, v5010 999 or v5010 271 if the request was a v5010 270).

4.3.1.2 Batch Submission

Batch requests are sent in the same way as real time requests. Batch requests are acknowledged using an HTTP/S acknowledgement and the envelope standard and metadata as specified in §4.4.

4.3.1.3 Batch Response Pickup

Batch responses are retrieved after the message receiver has had a chance to process a batch submission (see the CORE 155: Batch Response Time Rule version 1.1.0 and CORE 250 Claim Status Rule version 2.1.0, §4.5: Claim Status Response Time Requirements for details on timing.) Under this usage pattern, the message sender connects to the message

[23] MTOM is defined in Appendix §6.1: *Definitions and Abbreviations used in this Rule.*

receiver using HTTP/S with the envelope standard and metadata specified in §4.4, and sends a message requesting available files. The responder then sends back either:

1. The file(s) in the HTTP/S response message (payload) using the envelope standard and metadata specified in §4.4, or
2. A list of available file(s) in the HTTP/S response message (payload), and supports a mechanism to request a particular file from the list. If a Batch response contains a list of files, then the site's Connectivity Companion Guide (See §4.3.7) will specify the method to pick up each file in the list.

4.3.2 Submitter Authentication and Authorization Handling

The two methods for Submitter Authentication specified in this rule are:

1. Username/Password (Referred to as Submitter Authentication Standard C in the Conformance Requirements, §4.1) using the CORE-compliant Envelope to send the *UserName* and *Password*, as specified in the CORE-compliant Envelope Metadata specifications. For both envelope methods, the Username and Password are a part of the CORE-compliant envelope. For the SOAP+WSDL method, the WS-Security standard must be used to embed the Username and Password values inside the Envelope, as illustrated in the examples above.
2. X.509 Certificate based authentication over SSL[24] (Submitter Authentication Standard D in the Conformance Requirements, §4.1), using the Secure Sockets Layer (SSLv3.0) open standard for client certificate based authentication.

The submitter authentication conformance requirements for stakeholders are defined in §4.1.

Submitter Authorization is assumed to be a local decision at the site that receives the submission.

4.3.3 Error Handling

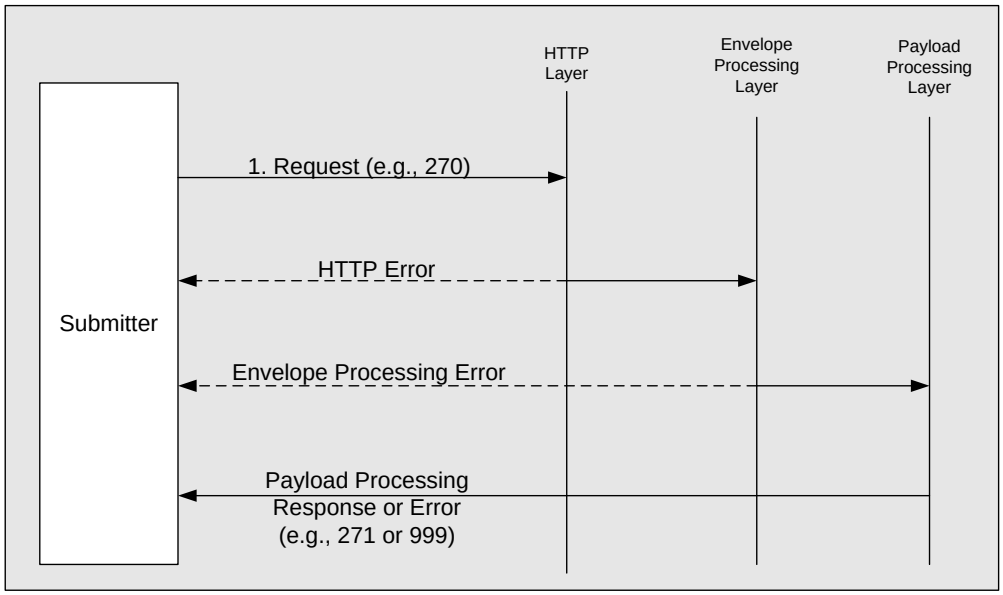
The error handling described in this section is applicable to both envelope methods. As shown in Figure #4.3.3 below, a submitted request goes through at least 3 logical layers that process the request.

- Processing of HTTP headers (typically handled by a web-server)
- Processing the Envelope (can be handled by messaging middle-ware or integration brokers)
- Processing the Payload (e.g., ASC X12, typically handled by application business logic)

Once a request (e.g., ASC X12 v5010 270) is submitted it goes through these 3 logical layers. At each of these layers, some part of the request is processed. At each layer there can be errors (indicated by the dotted arrows being returned to the request submitter), which may be returned to the request submitter. If there is an error in processing the message at any logical layer, the request does not get passed to the next layer. If no errors are encountered at that layer, the request is passed to the next processing layer. The last logical layer that processes the request is the Payload Processing Layer. Once this layer processes the payload, it returns a response or error (e.g., ASC X12 v5010 271 or v5010 999 or TA1).

[24] Reference §3.1 for more information regarding the use of SSL and the optional use of TLS 1.0.

Figure #4.3.3



Note: In Figure #4.3.3 above, the dotted line arrows indicate error messages being returned to the Submitter if there is a processing error at the corresponding logical processing layer. The straight line arrows indicate the request and response messages.

4.3.3.1 HTTP Status and Error Codes (Normative, Not Comprehensive[25])

The processing and error codes for the HTTP Layer are defined as part of the HTTP specifications [*http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*]. The intended use of these status and error codes in processing the requests are specified in Table 4.3.3.1 and are consistent with the HTTP status codes from CORE Phase I.

Note: The status and error codes included in Table 4.3.3.1 only represent a short list of several commonly used status codes in the standard. An exhaustive list of HTTP Status Codes and descriptions are included in the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1] Phase II CORE Connectivity requires the use of the appropriate HTTP error or status codes as applicable to the error/status situation.

Table 4.3.3.1

HTTP Status/Error Codes (Normative, Not Comprehensive)	**Status Code Description[26] (Intended Use)**
200 OK	Success
202 Accepted	Batch file submission has been accepted (but not necessarily processed)
400 Bad Request	Incorrectly formatted HTTP headers
403 Forbidden	Access denied (e.g., X.509 client certificate based authentication)[27]

[25] An exhaustive list of HTTP Status Codes and definitions are included in section 6.1.1 of the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1].
[26] Section 6.1.1 of the HTTP specification http://tools.ietf.org/html/rfc2616#section-6.1.1.

HTTP Status/Error Codes (Normative, Not Comprehensive)	Status Code Description[26] (Intended Use)
500 Internal Server Error	The web-server encountered a processing error, or there was a SOAP fault (in case of SOAP envelope method)
5xx Server errors	Standard set of server side errors (e.g., 503 Service Unavailable)

4.3.3.2 Envelope Processing Status and Error Codes (Normative, Comprehensive)

When SOAP is used, some of the CORE-compliant Envelope Processing errors map to SOAP faults [*http://www.w3.org/TR/soap12-part1/#soapfault*]. (See Table 4.3.3.2) To handle CORE-compliant envelope processing status and error codes, two fields called *ErrorCode* and *ErrorMessage* are included in the CORE-compliant Envelope. (See §4.4) *ErrorMessage* is a free form text field that describes the error (for the purpose of troubleshooting/logging). When an error occurs, *PayloadType* is set to *CoreEnvelopeError*.

Table 4.3.3.2

CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive)	Status Code Description[28] (Intended Use)
Success	Envelope was processed successfully.
<FieldName>Illegal	Illegal value provided for <FieldName>.
<FieldName>Required	The field <FieldName> is required but was not provided.
<FieldName>NotUnderstood	The field <FieldName> is not understood at the receiver. In the case of SOAP, this error is returned as a NotUnderstood SOAP fault.
VersionMismatch	The version of the envelope sent is not acceptable to the receiver. If the SOAP version is not valid at the receiver, a SOAP fault is returned with this fault code.
UnAuthorized	The username/password or Client certificate could not be verified.
ChecksumMismatched	The checksum value computed on the recipient did not match the value that was sent in the envelope.
Sender	The envelope sent by the sender did not conform to the expected format. In the case of SOAP, this error should be sent as a SOAP fault with "Sender" fault code.
Receiver	The message could not be processed for reasons attributable to the Receiver (e.g., upstream process is not reachable). In the case of SOAP, this error should be sent as a SOAP fault with "Receiver" fault code.

[27] If the username/password option is used, then these values are specified in the CORE-compliant envelope, which is not processed at the HTTP layer. This is handled by the error code (Unauthorized.)
[28] An exhaustive list of HTTP Status Codes and definitions are included in section 6.1.1 of the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1].

4.3.3.3 Examples of Status and Error Codes (non-normative)

The following illustrates the status and error codes that may be returned:

- A SOAP or MIME Multipart request that has illegal HTTP headers gets a response with HTTP Error Code: "400 Bad Request."
- A SOAP or MIME Multipart request with an unauthorized submitter's client-certificate (in case that method is being used) gets a response with HTTP Error Code: "403 Forbidden."
- A SOAP request with HTTP headers properly formatted but using the wrong SOAP version (1.1 instead of 1.2) gets HTTP Status 500, and a SOAP fault with a fault code "VersionMismatch."
- A MIME Multipart request with HTTP headers properly formatted, uses a properly formatted MIME Header but does not have *PayloadType* in the CORE-compliant envelope gets a HTTP Status 200 (since it passed the HTTP layer successfully), but receives an Envelope processing error with *ErrorCode* set to *PayloadTypeRequired*.
- A MIME Multipart request with HTTP headers properly formatted uses a properly formatted MIME Header but has *PayloadType* in the CORE-compliant envelope with an unknown value (i.e., not in the Coded Set defined for this field). This gets a HTTP Status 200 response (since it passed the HTTP layer successfully), but receives an Envelope processing error with *ErrorCode* set to *PayloadTypeIllegal.*

4.3.3.4 Examples of Error Messages (non-normative)

ErrorMessage field is intended to provide a descriptive text of the error message in free form text, to aid in logging and troubleshooting. It is the responsibility of the implementer to keep this message consistent with the semantics of the *ErrorCode*, and not in conflict with it. The *ErrorMessage* must be related to the *ErrorCode* as defined in the table above. The following illustrates *ErrorMessage* fields that may be returned:

- For *ErrorCode* = *VersionMismatch*, the *ErrorMessage* could be "Expecting CORERuleVersion=X, Received CORERuleVersion=Y"
- For *ErrorCode* = *SenderIDIllegal*, the *ErrorMessage* could be "SenderID length exceeds maximum allowed length"
- For *ErrorCode* = *TimeStampIllegal*, the *ErrorMessage* could be "Timestamp is missing the time-zone information"
- For *ErrorCode* = *CheckSumIllegal*, the *ErrorMessage* could be "Unknown algorithm", or "Unknown encoding type"
- For *ErrorCode* = *Receiver*, the *ErrorMessage* could be "Failed to connect to backend system X to process this message"

4.3.4 Audit Handling

Auditing is a local decision by each trading partner. The CORE recommended best practice is for each trading partner to audit all the envelope metadata and payload for each transaction.

4.3.4.1 Tracking of Date and Time and Payload ID

In order to comply with the Phase I CORE 155 and 156: Response Time Rules version 1.1.0 and Phase II CORE 250 Claim Status Rule, version 2.1.0, §4.4 and §4.5: Claim Status Response Time Requirements, 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, as specified in the CORE Envelope Metadata Table 4.4.2, message senders must include the date and time the message was sent in the CORE metadata element Time Stamp.

4.3.5 Capacity Plan

4.3.5.1 Real Time Transactions

A CORE-certified entity must have a capacity plan such that it can receive and process a large number of single concurrent real time transactions via an equivalent number of concurrent connections. These single transactions must be received, processed and the appropriate response provided back to the sender within response time requirements specified in Phase I CORE 156 Real Time Response Time Rule version 1.1.0 and Phase II CORE 250 Claim Status Rule version 2.1.0, §4.4: Real Time Response Time Requirements.

Three major factors affect the specific number of Large Volume of Single Real time Transactions (See §6.1) capable of being transported and processed within a given CORE response time frame. They are:

1. The amount of message metadata and message encapsulation structure which is required for each transaction;
2. The characteristics of the message handling software and how concise its design and coding are; and,
3. The architecture of the intervening hardware, software and communication platform.

CORE-certified entities must attest that their capacity planning addresses the above 3 factors that affect large volume single real time processing[29]. CORE-certified entities must also attest that they have the ability to track, on a calendar week basis, any change to their agreed upon volume capacity.

In the circumstances where the transaction volume throughput is exceeded by one of the trading partners, the receiving organization may declare a denial of service event and request a temporary waiver of the applicable CORE response time rule's performance criteria, and/or other appropriate action.

4.3.5.2 Batch Transactions

The CORE-certified messaging system must have the capability to receive and process large batch transaction files if the entity supports batch transactions. These transactions must be received, processed and the appropriate response provided back to the sender within the time specified in the applicable CORE Rule.

Three major factors that affect the specific number of Large Batch payloads capable of being transported and processed within a given time frame are:

1. The availability and use of capabilities in the messaging protocol which support in-line files, file attachments, and automated integrity assurance routines, etc., together with the quality and characteristics of their implementation;
2. The characteristics of the message handling software and its conciseness of design and coding; and,
3. The architecture of the intervening hardware, software and communication platform.

CORE-certified entities must attest that their capacity planning addresses the above 3 factors that affect large batch processing. The maximum number of transaction sets to be included in a large batch file is determined between trading partners.

4.3.6 Response, Timeout and Retransmission Requirements

- Real time response must conform to Phase I CORE 156 Eligibility and Benefits Real Time Response Time Rule version 1.1.0.
- Batch response time must conform to Phase I CORE 155 Eligibility and Benefits Batch Response Time Rule version 1.1.0.

If a Real time response message is not received within the 60 second response period, the submitter's system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

[29] See *Appendix 6.1: Abbreviations and Definitions used in this Rule* for a definition of Large Volume of Single Real time Transactions (Synchronous).

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

If additional attempts result in the same timeout termination, the submitter's system must notify the submitter to contact the receiver directly to determine if system availability problems exist or if there are known Internet traffic constraints causing the delay.

4.3.7 Publication of Entity-Specific Connectivity Guide

Servers must publish detailed specifications in a Connectivity Companion Guide on the entity's public web site. CORE recommends specifying the following:

- CORE Rule Version for Connectivity.
- Details on the message format and the supported transactions (e.g., Real time, Batch transactions).
- Details about the entity's ASC X12 Interchange; e.g., will an interchange contain multiple functional groups; will the TA1 be in its own interchange without any functional group(s).
- An entity may implement custom extensions which are not compliant with the CORE Connectivity Rule. Any such extension must be specified in the entity's companion guide. Consistent with the CORE Safe Harbor principle (§5 Safe Harbor), a CORE certified entity can implement custom extensions and/or support additional connectivity methods as long as the organization has implemented one connectivity interface that is fully and exactly as specified in the CORE Connectivity Rule. This gives CORE certified partners the assurance that they can use their CORE Connectivity-certified interfaces.
- If a Batch response contains a list of files (instead of returning the Batch file itself), the location and mechanism to pick up each file in that list (e.g., FTP, HTTP, or Web-Service) should be specified in the entity's Connectivity Companion Guide.. When a Batch response contains a list of files, it is an example of a custom extension that is considered outside of the CORE Safe Harbor.
- Value of *ReceiverID* for that site.
- Production and Testing URLs for Real time and Batch transactions.
- Maximum number of Real time and Batch transactions that can be sent per minute by a single trading partner (Client).
- Maximum size of Batch files that can be received by a Server.
- Authentication/Authorization policies using either X.509 Client Certificates or User ID and Password (e.g., how to enroll and obtain a Client Certificate or *UserID* and *Password* to connect to that Receiver).
- Information on obtaining the Receiver's Root Certificate Authority and/or Intermediate Certificate Authority public key certificate.
- System Availability as required by Phase I CORE 157 System Availability Rule version 1.1.0 and Phase II CORE 250 Claim Status Rule version 2.1.0, §4.6: Claim Status System Availability.
- Business/Technical points of contact.
- Rules of behavior for programs that connect to this site (e.g., must not deliberately submit batch files that contain Viruses).

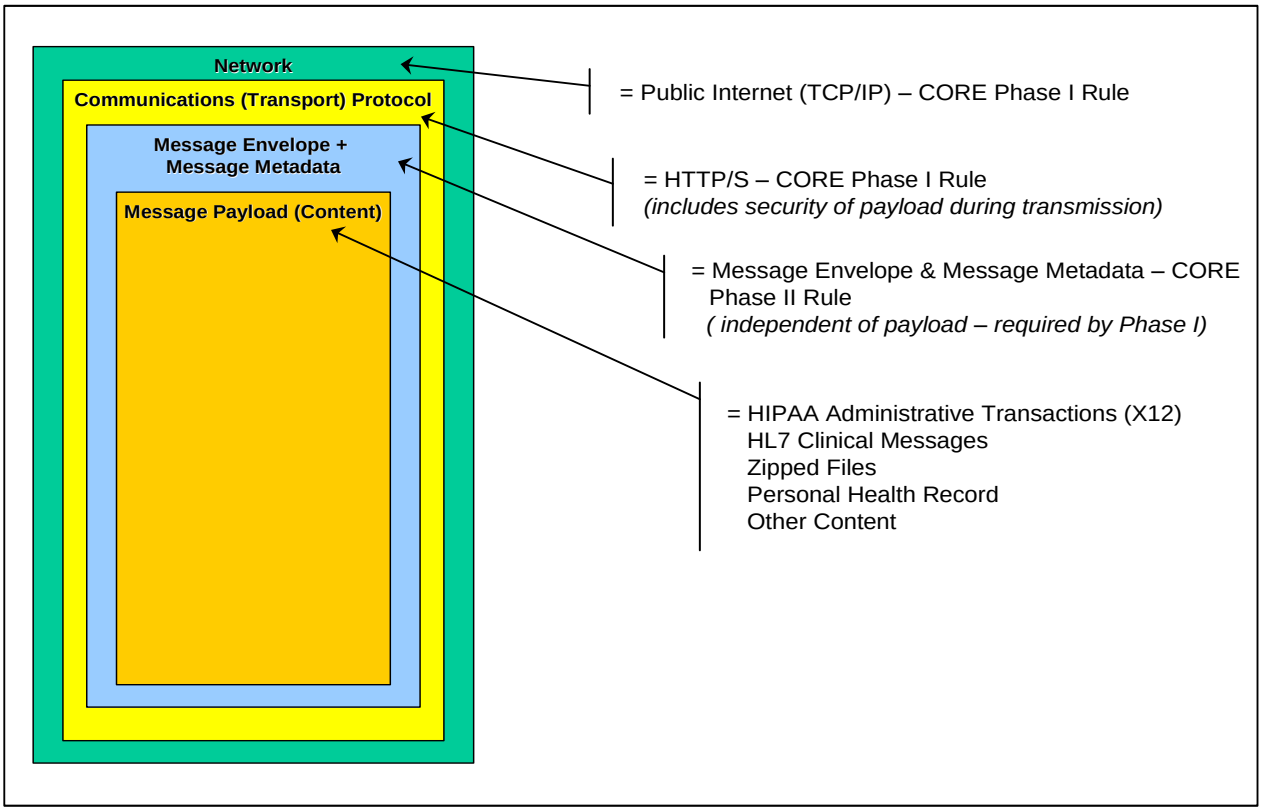
4.4 Envelope Metadata Fields, Descriptions, Intended Use and Syntax/Value-Sets

The Envelope Metadata specified in Table 4.4.2 on the following page pertains to the Phase II Message Envelope identified in §4.4.1, and is applicable to both enveloping standards (SOAP+WSDL and HTTP MIME Multipart) that may be used for encoding the Phase II message envelope (subject to the conformance requirements discussed in the Conformance section of this rule). With the exception of *ErrorCode* and *ErrorMessage* fields, which are only sent in the response, the CORE Phase II-required envelope metadata for the request and response are required to be identical.

4.4.1 Message Envelope

As shown in Figure #4.4.1 below, the Message Envelope is outside the Message Payload (content), and inside the transport protocol envelope. The Phase I CORE 153 Connectivity Rule version 1.1.0 was based on the use of HTTP/S as the transport protocol; hence the transport protocol envelope consists of HTTP headers. Examples of message payload include HIPAA administrative transactions (ASC X12), HL7 clinical messages, zipped files, etc.

Figure #4.4.1



4.4.2 Table of CORE Envelope Metadata

Non-normative (Descriptive)			Normative (Definitive)			
Element	**Description**	**Expected Use**	**Field Name[30]**	**Requirement Indicator for Real Time and Batch**	**Data Type**	**Field Constraints or Value-sets (Not comprehensive)**
Payload Type	Payload Type specifies the type of payload included within a request, (e.g. HIPAA X12 transaction set 270, 276, 278, etc.).	• Message routing • Efficient processing • Auditing	PayloadType	Required for both	Coded Set	Please see §4.4.3 for enumeration of PayloadType field.
Processing Mode	Processing Mode indicates Batch or Real time[31] processing mode (as defined by CORE)	• Messaging routing • Resource allocation • Transaction scheduling • Message or transaction auditing	ProcessingMode	Required for both	Coded Set	RealTime, Batch
Payload Length	Defines the length of the actual payload in bytes.	• Efficient processing and resource allocation. • Auditing • Trouble-shooting	PayloadLength	Required for Batch interactions except under certain conditions[32] Shall not be used for Real time.	Integer (Base 10)	
Payload ID	Payload ID (unique within the domain of the party that sets this value) is a payload identifier assigned by the Sender in both Batch and Real Time processing modes. If the payload is being resent in the absence of confirmation of receipt to persistent storage, the same PayloadID may be re-used.	• Auditing • Trouble-shooting	PayloadID	Required for both Real time and Batch.	String	*PayloadID* will conform to ISO UUID standards (described at ftp://ftp.rfc-editor.org/in-notes/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address[33], to ensure uniqueness.

[30] Mixed case (e.g., *PayloadType*) is used for the field names, since this is consistent with the WS-Security tags that are used for authentication.
[31] See *Appendix 6.1: Abbreviations and Definitions used in this Rule* for a definition of Batch and Real time.
[32] Some requests or responses within Batch interactions may not have a payload. This could occur when requesting a payload or when there is no payload in the response.
[33] In multithreaded environments, in addition to the hardware (MAC) address and timestamp, the Process-ID or Thread-ID may also be used as additional parameters to ensure *PayloadID* uniqueness across multiple processes and/or threads.

Non-normative (Descriptive)			Normative (Definitive)			
Element	**Description**	**Expected Use**	**Field Name[30]**	**Requirement Indicator for Real Time and Batch**	**Data Type**	**Field Constraints or Value-sets (Not comprehensive)**
Time Stamp (Adjusted from Phase I)	The Sender (request) or Receiver (response) Time Stamp combines Phase I time and date[34] message metadata into a single Coordinated Universal Time (UTC) time stamp (including time zone information) specifying when a message is created and sent to a receiver. This does not require a shared time server for consistent time.	• Auditing • Trouble-shooting	TimeStamp	Required for both	dateTime	dateTime (http://www.w3.org/TR/xmlschema11-2/#dateTime)
User Name[35] (Already in Phase I)	User Name is part of User Name/Password based authentication credentials. It can also be used by the receiver for authorization purposes. User Name is protected by transport layer SSL[36] encryption. User Name must be used only for identification, authentication and authorization purposes while Sender Identifier must be used to identify trading partners and convey other business information within a transaction.	• Authentication and authorization • Auditing	UserName	Required for both if X.509 Client-certificate authentication over SSL/TLS[37] is not used.	String	Maximum length 50 characters
Password (Already in Phase I)	Password is part of the User Name/Password based authentication credentials. Password is protected by transport layer SSL[38] encryption.	Submitter Authentication	Password	Required for both if X.509 Client-certificate authentication over SSL/TLS is not used. If UserName field is present, a corresponding Password must be present.	String	Maximum length 50 characters

[34] See CORE Phase I Connectivity Rule for time, date message metadata requirements.
[35] See CORE Phase I Connectivity Rule for User ID and Password as part of the Security and Authentication Requirements.
[36] Reference §3.1 for more information regarding the use of SSL and the optional use of TLS 1.0.
[37] This type of authentication is consistent with the IHE's Audit Trail and Node Authentication (ATNA) profile.
[38] Reference §3.1 for more information regarding the use of SSL and the optional use of TLS 1.0.

Non-normative (Descriptive)			Normative (Definitive)			
Element	**Description**	**Expected Use**	**Field Name[30]**	**Requirement Indicator for Real Time and Batch**	**Data Type**	**Field Constraints or Value-sets (Not comprehensive)**
Sender Identifier	A unique[39] business entity identifier representing the message envelope creator. Sender Identifier is better suited for identifying business entities and trading partners than User Name because: • User Name is usually anonymized for security reasons and to protect privacy. • User Name attribute does not exist if another authentication method is used. • Authentication and messaging may happen on different layers[40] and therefore may be handled by disparate applications and processes.	• Message routing and processing by a receiver • Transaction auditing. • As a reference to a business agreement.	SenderID	Required	String	Maximum length 50 characters The use of OIDs (e.g., HL7 or IANA) is recommended, but not required.
Receiver Identifier	A unique[41] business entity identifier representing the next-hop receiver.	• Transaction auditing. • As a reference to a business agreement. • Message routing by the receiver.	ReceiverID	Required	String	Maximum length 50 characters The use of OIDs (e.g., HL7 or IANA) is recommended, but not required.
CORE Rule Version	The CORE Rule version that this envelope is using. This value can be used to maintain backward compatibility when parsing/processing messages. A Phase II certified receiver must be able to interact with both Phase I and Phase II certified senders for backward compatibility.	• Message routing and processing. • Auditing • Backward compatibility.	CORERuleVersion	Required for both	Coded Set	2.2.0

[39] Unique within the Sender's domain.
[40] §2 shows the layers in the OSI model.
[41] Unique within a Receiver's domain.

Non-normative (Descriptive)			Normative (Definitive)			
Element	**Description**	**Expected Use**	**Field Name[30]**	**Requirement Indicator for Real Time and Batch**	**Data Type**	**Field Constraints or Value-sets (Not comprehensive)**
Checksum	An element used to allow receiving site to verify the integrity of the message that is sent.	Message Integrity verification	CheckSum	Required for Batch interactions except under certain conditions[42] Not used for Real time	String	Algorithm is SHA-1, Encoding is Hex. Checksum must be computed only on the payload and not on the metadata.
Error Code	Error code to indicate the error when processing the envelope.	• Error handling • Troubleshooting	ErrorCode	Required in Response (for both Real time and Batch) Not used in Request.	Coded Set	Please see Section on Error Handling for a definition of error codes.
Error Message	Text Error message that describes the condition that caused the error. The text of the *ErrorMessage* must provide additional information describing how the Error can be resolved, and must not provide conflicting information from that provided in the *ErrorCode*.	• Logging • Troubleshooting	ErrorMessage	Required in Response (for both Real time and Batch) Not used in Request	String	Maximum length of 1024 characters. Please see Section on Error Handling for examples of Error Messages.

[42] Some requests or responses within Batch interactions may not have a payload. This could occur when requesting a payload or when there is no payload in the response.

4.4.3 Enumeration of Processing Mode and PayloadType Fields

4.4.3.1 Real Time Transactions

For Real time requests, *ProcessingMode* must be set to *RealTime,* and *PayloadType* must be set to the following values for Request, Response and Errors.

Payloads to Support All ASC X12 Administrative Transactions for Real Time					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[43]		**V5010**	
		Request	**Response**	**Request**	**Response**
Health Care Eligibility Benefit Inquiry and Response	Y	X12_270_Request_004010X092A1	X12_271_Response_004010X092A1	X12_270_Request_005010X279A1	X12_271_Response_005010X279A1
Health Care Claim Status Request and Response	Y	X12_276_Request_004010X093A1	X12_277_Response_004010X093A1	X12_276_Request_005010X212	X12_277_Response_005010X212
Health Care Services Request for Review and Response	Y	X12_278_Request_004010X094A1	X12_278_Response_004010X094A1	X12_278_Request_005010X217E1_2	X12_278_Response_005010X217E1_2
Health Care Services Review - Inquiry & Response	N	X12_278_Request_004010X059	X12_278_Response_004010X059	X12_278_Request_005010X215	X12_278_Response_005010X215
Health Care Services Review - Notification & Announcement	N	X12_278_Request_004010X111	X12_278_Response_004010X111	X12_278_Request_005010X216E2	X12_278_Response_005010X216E2
Real Time Adjudication					
Health Care Claim: Institutional	N			X12_837_ Request_005010X223A1_2	X12_835_ Response_005010X221A1
Health Care Claim: Professional	N			X12_837_ Request_005010X222A1	X12_835_ Response_005010X221A1
Health Care Claim: Dental	N			X12_837_ Request_005010X224A1_2	X12_835_ Response_005010X221A1

[43] Several PayloadType values referencing version 004010 of various administrative transactions are being retained since these implementation guides are not adopted under HIPAA. As such, the industry may continue using these implementation specifications to support their business needs and are not required to move to a 5010 version of them. The corresponding v5010 implementation guides have been added to the value set to support the industry's transition to v5010 in general.

Payloads to Support All ASC X12 Administrative Transactions for Real Time					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[44]		**V5010**	
		Request	**Response**	**Request**	**Response**
Acknowledgements					
TA1 Interchange Acknowledgement	N		X12_TA1_Response_00401[45]		X12_TA1_Response_00501X231A1[46]
Functional Acknowledgement	N		X12_997_Response_004010		
Implementation Acknowledgement	N				X12_999_Response_005010X231A1
Errors					
CORE Envelope Error	N/A		CoreEnvelopeError		CoreEnvelopeError

[44] Several PayloadType values referencing version 004010 of various administrative transactions are being retained since these implementation guides are not adopted under HIPAA. As such, the industry may continue using these implementation specifications to support their business needs and are not required to move to a 5010 version of them. The corresponding v5010 implementation guides have been added to the value set to support the industry's transition to v5010 in general.

[45] The use of the TA1 Interchange Acknowledgement is not specified in a separate ASC X12 Implementation Specification. Reference Appendix B EDI Control Directory of the ASC X12N v4010 Implementation Guide for technical details of the TA1. Reference Appendix C EDI Control Directory of the ASC X12C 005010231A1 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 for implementation guidance of the TA1 with v5010 ASC X12 administrative transactions.

[46] Ibid.

4.4.3.2 Batch Transactions

For Batch requests, *ProcessingMode* must be set to *Batch*, and *PayloadType* must be set to the following values for Request, Response and Errors.

Payloads to Support All ASC X12 Administrative Transactions for Batch					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[47]		**V5010**	
		Request	**Response**	**Request**	**Response**
Batch Payload (Submission and Subsequent Batch Response Pick Up) See §6.3.2 Batch Interaction					
Health Care Eligibility Benefit Inquiry and Response	Y	Batch Submission: X12_270_Request_004010X092A1 Results Retrieval Request: X12_004010_Request_BatchResults271	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_271_Response_004010X092A1	Batch Submission: X12_270_Request_005010X279A1 Results Retrieval Request: X12_005010_Request_Batch_Results_271	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_271_Response_005010X279A1
Health Care Claim Status Request and Response	Y	Batch Submission: X12_276_Request_004010X093A1 Results Retrieval Request: X12_004010_Request_BatchResults277	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_277_Response_004010X093A1	Batch Submission: X12_276_Request_005010X212 Results Retrieval Request: X12_005010_Request_Batch_Results_277	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_277_Response_005010X212
Health Care Services Request for Review and Response	Y	Batch Submission: X12_278_Request_004010X094A1 Results Retrieval Request: X12_278_Request_Batch_Results_004010X094A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_004010X094A1	Batch Submission: X12_278_Request_005010X217E1 Results Retrieval Request: X12_278_Request_Batch_Results_005010X217E1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_005010X217E1
Health Care Services Review - Inquiry & Response	N	Batch Submission: X12_278_Request_004010X059 Results Retrieval Request: X12_278_Request_Batch_Results_004010X094A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_004010X059	Batch Submission: X12_278_Request_005010X215E1 Results Retrieval Request: X12_278_Request_Batch_Results_005010X215E1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_005010X215E1
Health Care Services Review - Notification & Announcement	N	Batch Submission: X12_278_Request_004010X111 Results Retrieval Request: X12_278_Request_Batch_Results_004010X111	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_004010X111	Batch Submission: X12_278_Request_005010X216E1_2 Results Retrieval Request: X12_278_Request_Batch_Results_005010X216E1_2	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Results Retrieval Response: X12_278_Response_005010X216E1_2
Batch Payload (Pick Up only) See §6.3.3 Generic Batch Retrieval Request and Asynchronous Receipt Confirmation					
Health Care Claim Acknowledgement	N			Retrieval Request: X12_277CA_Request_005010X214E1_2	Retrieval Response: X12_277CA_Response_005010X214E1_2
Health Care Claim Payment/Advice	Y	Retrieval Request: X12_835_Request_004010X091A1	Retrieval Response: X12_835_Response_004010X091A1	Retrieval Request: X12_835_Request_005010X221A1	Retrieval Response: X12_835_Response_005010X221A1
Health Care Claim Pending Status Information	N			Retrieval Request: X12_277_Request_005010X228E1	Retrieval Response: X12_277_Response_005010X228E1

[47] Several PayloadType values referencing version 004010 of various administrative transactions are being retained since these implementation guides are not adopted under HIPAA. As such, the industry may continue using these implementation specifications to support their business needs and are not required to move to a 5010 version of them. The corresponding v5010 implementation guides have been added to the value set to support the industry's transition to v5010 in general.

Payloads to Support All ASC X12 Administrative Transactions for Batch					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[47]		**V5010**	
		Request	**Response**	**Request**	**Response**
Batch Payload (Submission of Payload followed by Submission of Results) See §6.3.4 Generic Batch Submission and Synchronous Receipt Confirmation					
Health Care Claim Request for Additional Information	N			Batch Submission (step 1): X12_277_Request_005010X213E1_2 Batch Submission (step 2): X12_275_Request_005010X210E1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Acknowledgement: X12_TA1_Response_00501X231A or X12_999_Response_005010X231A1
Request for Information in Support of a Disability Claim	N			Batch Submission (Step 1): X12_277_Request_005010X227 Batch Submission (Step 2) X12_275_Request_005010X210E1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation Acknowledgement: X12_TA1_Response_00501X213A or X12_999_Response_005010X231A1
Batch Payload (Submission only) See §6.3.4 Generic Batch Submission and Synchronous Receipt Confirmation					
Health Care Claim: Institutional	Y	Batch Submission: X12_837_Request_004010X096A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation	Batch Submission: X12_837_Request_005010X223A1_2	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Health Care Claim: Professional	Y	Batch Submission: X12_837_Request_004010X098A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation	Batch Submission: X12_837_Request_005010X222A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Health Care Claim: Dental	Y	Batch Submission: X12_837_Request_004010X097A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation	Batch Submission: X12_837_Request_005010X224A1_2	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Payroll Deducted and Other Group Premium Payment for Insurance Products	Y	Batch Submission: X12_820_Request_004010X061A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation	Batch Submission: X12_820_Request_005010X218A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Benefit Enrollment and Maintenance	Y	Batch Submission: X12_834_Request_004010X095A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation	Batch Submission: X12_834_Request_005010X220A1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Health Care Benefit Coordination Verification	N			Batch Submission: X12_269_Request_005010X187	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Health Care Predetermination – Professional	N			Batch Submission: X12_837_Request_005010X291	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Health Care Predetermination – Institutional	N			Batch Submission: X12_837_Request_005010X292	Batch Receipt Confirmation: X12_BatchReceiptConfirmation
Doctors First Report of Injury	N	Batch Submission: X12_148_Request_004010X148	Batch Receipt Confirmation: X12_BatchReceiptConfirmation		
Health Care Service: Data Reporting	N			Batch Submission: X12_837_Request_005010X225A1_2E1	Batch Receipt Confirmation: X12_BatchReceiptConfirmation

Payloads to Support All ASC X12 Administrative Transactions for Batch					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[48]		**V5010**	
		Request	**Response**	**Request**	**Response**
Mixed/Non-Payload Specific Batch See §6.3.2 Batch Interaction					
Batch Submission (mixed payload types)	N/A	X12_004010_Request_BatchSubmissionMixed	X12_004010_Response_BatchSubmissionMixed	X12_005010_Request_BatchSubmissionMixed	X12_005010_Response_BatchSubmissionMixed
Batch Results Retrieval (mixed payload types)	N/A	X12_004010_Request_BatchResultsMixed	X12_004010_Response_BatchResultsMixed	X12_005010_Request_BatchResultsMixed	X12_005010_Response_BatchResultsMixed
No Batch Results Available	N/A		X12_004010_Response_NoBatchResultsFile		X12_005010_Response_NoBatchResultsFile
Acknowledgements					
Batch Receipt Confirmation Response	N		X12_BatchReceiptConfirmation		X12_BatchReceiptConfirmation
TA1 Interchange Acknowledgement Submission	N	X12_TA1_SubmissionRequest_00401[49]	X12_Response_ConfirmReceiptReceived	X12_TA1_SubmissionRequest_00501X231A1[50]	X12_Response_ConfirmReceiptReceived
Retrieval of TA1	N	X12_TA1_RetrievalRequest_00401	X12_TA1_Response_00401[51]	X12_TA1_RetrievalRequest_00501X231A1	X12_TA1_Response_00501X231A1[52]
997 Functional Acknowledgement Submission	N	X12_004010_SubmissionRequest_997	X12_Response_ConfirmReceiptReceived		
Retrieval of 997	N	X12_997_RetrievalRequest_00401	X12_004010_Response_997		
Implementation Acknowledgement Submission	N			X12_999_SubmissionRequest_005010X231A1	X12_Response_ConfirmReceiptReceived
Implementation Acknowledgement Retrieval	N			X12_999_RetrievalRequest_005010X231A1	X12_999_Response_005010X231A1
Application Reporting for Insurance	N			X12_824_Request_005010X186	X12_824_Response_005010X186

[48] Several PayloadType values referencing version 004010 of various administrative transactions are being retained since these implementation guides are not adopted under HIPAA. As such, the industry may continue using these implementation specifications to support their business needs and are not required to move to a 5010 version of them. The corresponding v5010 implementation guides have been added to the value set to support the industry's transition to v5010 in general.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.

Payloads to Support All ASC X12 Administrative Transactions for Batch					
Transaction Name	**HIPAA Mandated**	**Payload Type Value (Normative/Comprehensive)**			
		V4010A1[53]		**V5010**	
		Request	**Response**	**Request**	**Response**
Acknowledgements (Continued)					
General Acknowledgements Pick Up	N	X12_004010_Request_Acks	X12_004010_Response_Acks	X12_005010_Request_Acks	X12_005010_Response_Acks
No Acknowledgement File	N/A		X12_004010_Response_NoBatchAckFile		X12_005010_Response_NoBatchAckFile
Payload Receipt Confirmation	N/A	X12_Request_ConfirmReceipt	X12_Response_ConfirmReceiptReceived	X12_Request_ConfirmReceipt	X12_Response_ConfirmReceiptReceived
Errors					
CORE Envelope Error	N/A		CoreEnvelopeError		CoreEnvelopeError

[53] Several PayloadType values referencing version 004010 of various administrative transactions are being retained since these implementation guides are not adopted under HIPAA. As such, the industry may continue using these implementation specifications to support their business needs and are not required to move to a 5010 version of them. The corresponding v5010 implementation guides have been added to the value set to support the industry's transition to v5010 in general.

4.4.4 Enumeration Convention for PayloadType when Handling Non-X12 Payloads (Non-normative)

The Envelope metadata specification in §4.4.3 includes a PayloadType field that is enumerated for X12 payload types. This envelope may also be used to transport other types of payloads. In such cases, the convention for the *PayloadType* field is as follows:

<SDO>_<PayloadType>_<Version>_<Sub-version>

Note: SDO stands for Standards Development Organization.

For example, an NCPDP based NEWRX SCRIPT Standard Implementation Guide Version 8.1 transaction of NEWRX payload may specify *PayloadType* as *NCPDP_NEWRX_008_001*, an HL7 based ADT04 Version 2.3.1 payload may specify the *PayloadType* as *HL7_ADT04_2_3_1*.

5 CORE SAFE HARBOR

The Phase I CORE 153 Connectivity Rule version 1.1.0 provided a "Safe Harbor" that application vendors, providers, and health plans (or other information sources) could be assured would be supported by any CORE-certified trading partner. This Phase II Connectivity Rule extends the Safe Harbor by further specifying the connectivity that all CORE-certified organizations must implement and with which conformance must be demonstrated. As such, in the Phase I rule:

- **DOES NOT** require trading partners (e.g., a provider or a health plan) to discontinue using existing connections that do not match the rule.
- **DOES NOT** require that trading partners must use a CORE-complaint method for all new connections.
- **DOES NOT** require all CORE trading partners use only one method for any connections.
- **DOES NOT** require CORE-certified entity to do business with any trading partner or other CORE-certified entity.

CORE expects that in some circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than those described in this rule to achieve the technical goals of the specific connection.

However, this Safe Harbor is the connectivity mechanism that a CORE-certified entity MUST use if requested by a trading partner. If the CORE-certified entity does not believe that this CORE Safe Harbor is the best connectivity mechanism for that particular trading partner, it may work with its trading partner to implement a different, mutually agreeable connectivity method. However, if the trading partner insists on using this Safe Harbor, the CORE-certified entity must accommodate that request. This clarification is not intended in any way to modify entities' obligations to exchange electronic transactions as specified by HIPAA or other federal and state regulations.

6 APPENDIX

6.1 Abbreviations and Definitions Used in this Rule

Term or Concept	Definition
ASC X12 Interchange	An ASC X12 Interchange is a graphic character string structured using delimited, tagged data concepts. An ASC X12 Interchange begins with an Interchange Control Header segment: Segment ID = ISA and ends with an Interchange Control Trailer segment: Segment ID – IEA. An ASC X12 Interchange may be composed of one or more Functional Groups (GS/GE Control Segments). An ASC X12 Functional Group is composed of one or more Transaction Sets (ST/SE Control Segments). An ASC X12 Interchange may be a Logical file or a physical file as determined by the originator of the Interchange. As such, a physical file may consist of one or more ASC X12 Interchanges. The ISA Interchange Control Header segment does not identify the content of any included Functional Groups. The Functional Group Control Header segment identifies the transaction set(s) in the Functional Group: GS08-480 Version/Release/Industry Indicator Code.
Asynchronous	A message exchange interaction is said to be asynchronous when the associated messages are chronologically and procedurally decoupled, e.g., in a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to do this include polling, notification by receipt of another message, etc. [WS Glossary, 2004]
Batch (Batch Mode, Batch Processing Mode)	Batch Mode is when the initial (first)[54] communications session is established and maintained open and active only for the time required to transfer a batch file of one or more transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses. Batch Processing Mode[55] is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling; notification by receipt of another message; or receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc. Batch, (asynchronous) Processing Mode is from the perspective of the request initiator. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.
Batch Files (Payload)	A single submission of a message payload that contains one X12 Interchange containing one Functional Group containing one X12 transaction set consisting of more than one business transaction.
Client	An entity that sends/relays a message to a Server.
CORE Safe Harbor	The connectivity requirements that application vendors, providers, and health plans (or other information sources) are required to support in order to provide assurance that these requirements are supported by any CORE-certified trading partners.[56]

[54] CORE Phase I Glossary Definitions. http://www.caqh.org/pdf/COREPIGlossary.pdf
[55] CORE Phase I Glossary Definitions. http://www.caqh.org/pdf/COREPIGlossary.pdf
[56] CORE Phase I Rule 153: Eligibility and Benefits Connectivity Rule Version 1.0.0

Term or Concept	Definition
Extensibility	Extensibility is a property of a system, format, or standard that allows evolution in performance or format within a common framework, while retaining partial or complete compatibility among systems that belong to the common framework.[57] Extensibility is a system design principle where the implementation takes into consideration future growth. It is a systematic measure of the ability to extend a system and the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality. The central theme is to provide for change while minimizing the impact to existing system functions.[58]
Federal Information Processing Standards Security Requirements for Cryptographic Modules (FIPS 140-2)	The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).
HTTP	Hypertext Transport Protocol Version 1.1 (IETF RFC 2616: http://www.ietf.org/rfc/rfc2616.txt).
HTTP MIME Multipart	MIME Multipart/related Content-type (IETF RFC 2388: http://www.ietf.org/rfc/rfc2388.txt).
Interoperability	Interoperability is the capability of different information technology systems, software applications and networks to communicate, execute programs, exchange data accurately, effectively and consistently, among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units and to use the information that has been exchanged.[59] Interoperability also requires no specific architecture and is independent of vendors and their various operating systems, programming languages, hardware, and network infrastructure. Functional interoperability is the capability to reliably exchange information without errors. Semantic interoperability allows systems to interpret and make effective use of the information exchanged among systems[60].

[57] http://www.atis.org/glossary/definition.aspx?id=7853 ATIS (Alliance for Telecommunications Industry Solutions http://www.atis.org/about/index.asp
[58] http://en.wikipedia.org/wiki/Extensibility
[59] Adapted from http://engineers.ihs.com/document/abstract/AQSBFBAAAAAAAAAA ANSI Information Technology – Vocabulary – Part 1: Fundamental Terms
[60] HIMSS Position Statement: Adoption of HITSP Interoperability Specifications July 2007

Term or Concept	Definition
Interoperability Specification[61]	An Interoperability Specification focuses on a set of constrained standards for information interchange that address the core requirements of the Use Cases. It does not define all functions, constructs and standards necessary to implement a conforming system in the real world environment. An Interoperability Specification defines how two or more systems exchange standard data content in a standard manner. Interoperability Specifications define the necessary business and technical actors, the transactions between them including the message, content and terminology standards for the actual information exchange. Interoperability Specifications do not specify the functional requirements or behaviors of the systems or applications. Interoperability Specifications, unless otherwise noted, are not intended to define or prescribe any system architecture or implementation. At the most basic level, the Interoperability Specifications define specific information exchange standards that are to be used by any two systems. Information exchange must be placed within the context of a transaction between defined technical actors which fulfill higher level business requirements derived from the use cases. In some cases the necessary technical actors may require some architectural structure or make some assumptions involving synchronous or asynchronous data exchanges, or require specific type of exchange, such as a message or document. These requirements may constrain to some degree the total range of choices regarding system architectures. When constraints are necessary to meet the use case requirements, the Interoperability Specification will note this and will retain as much architectural neutrality as possible. When appropriate, Interoperability Specifications may provide architectural examples and discuss considerations of such examples. HITSP and ONC do not define "Interoperability," but, do define "Interoperability Specification."
Large Batch Files (Payload)	A single submission of a message payload that contains more than one ASC X12 Interchange, each of which may contain one or more Functional Groups, each of which may contain one or more ASC X12 transaction sets.
Large Volume of Single Real time Transactions (Synchronous)	A high number of Real time transactions arriving at the receiving system concurrently. CORE defines large volume as "X"% of an organization's average daily received transaction volume (based on all trading partners) within one minute. "X" is defined by organization.
Message Encapsulation Layer	This refers to the Open Systems Interconnect (OSI) layers 5 and 6.
Message Envelope Standard A	HTTP MIME Multipart, described in Section "Specifications for HTTP MIME Multipart".
Message Envelope Standard B	SOAP+WSDL, described in Section "Specifications for SOAP + WSDL".
MIME	Multipurpose Internet Message Extensions (IETF RFCs 2045 to RFC 2049) [http://www.ietf.org/rfc/rfc2045.txt].
MTOM	W3C Message Transmission Optimization Mechanism (http://www.w3.org/TR/soap12-mtom/).
Normative	In standards terminology, "normative" means "considered to be a prescriptive part of the standard" [Wikipedia].

[61] HITSP Interoperability Specification: EHR Lab Terminology Component HITSP/ISC-35 October 20, 2006 Version 1.2

Term or Concept	Definition
Non-normative	Informational, not intended to be part of the specification.
OSI	Open Systems Interconnection Basic Reference Model (OSI Reference Model, or OSI Model for short) is a layered, abstract description for communications and computer network protocol design. From top to bottom, the OSI Model consists of the Application, Presentation, Session, Transport, Network, Data Link and Physical Layers [Wikipedia].
Open Standard [62]	"Open Standards" are those standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.
Payload	The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination. A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).[63]
Performance	According to CORE's Phase I Connectivity Rule, performance is defined in only two components: Response time – the time required to receive an Eligibility Request, process it completely and send an appropriate response, as specified in CORE's Phase I Eligibility and Benefits Rules and Policies for Real time [64] and Batch [65] exchanges. System Availability – the time an information source's (health plan, clearinghouse/switch or other intermediary system) processing system is capable of properly processing Eligibility Request/Response transactions, as specified in CORE's Phase I Eligibility and Benefits Rules and Policies for system availability[66].
Performance Evaluation Criteria	For the purpose of evaluating the measurable performance dimensions of potential messaging methodologies to be used in Real time healthcare transactions, Performance Evaluation Criteria may include: Response Time – the time required to receive an Eligibility Request, process it completely, and send an appropriate response.[67] Maximum Arrival Rate Before Saturation – the maximum number of properly formed arriving Eligibility Request transactions per time period (usually seconds or minutes), above which the ability for increased acceptance for further processing stops.[68] Overhead Information – Digital information transferred across the functional interface between a user and a telecommunications system, or between functional units within a telecommunications system, for the purpose of directing or

[62] International Telecommunication Union – Open Standards Definition. http://www.itu.int/ITU-T/othergroups/ipr-adhoc/openstandards.html
[63] SearchSecurity.com. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214475,00.html
[64] CORE Phase I 156: Eligibility and Benefits Real Time Response Time Rule
[65] CORE Phase I 155: Eligibility and Benefits Batch Response Time Rule
[66] CORE Phase I 157: Eligibility and Benefits System Availability
[67] CORE Phase I 156: Eligibility and Benefits Real Time Response Time Rule; and CORE Phase I 155: Eligibility and Benefits Batch Response Time Rule
[68] http://www.cs.washington.edu/homes/lazowska/qsp/Contents.pdf Quantitative System Performance, Chapter 5.2.1. Transaction Workloads (Page 72)

Term or Concept	Definition
	controlling the transfer of user information or the detection and correction of errors. Note: Overhead information originated by the user is not considered to be system overhead information. Overhead information generated within the communications system and not delivered to the user is system overhead information. Thus, the user throughput is reduced by both overheads while system throughput is reduced only by system overhead.[69] Capacity – the maximum number of completed Eligibility Request/ Response transaction sets per specific time period. Quality of Service – the number of properly and accurately completed Eligibility Request/Response transaction sets divided by the number of properly submitted transactions (Requests). When making such performance measurements and evaluations, it is important to consider the architecture of networks and systems to assure their similarity, and/or to assess the relevance and impact of any differences.
Real time (Real time Mode, Real time Processing Mode) [70]	Real time Mode [71] is when an entity is required to immediately send a single transaction and receive a single, related response within a single communications session, which is established and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed. Real time Mode & Real time Processing Mode are also considered to be a synchronous processing mode. (See Synchronous). Real time, or synchronous, Processing Mode is from the perspective of the request initiator.
Safe Harbor	A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[72] In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.
Secure Sockets Layer (SSL)	See Transport Layer Security.
Server	An entity that receives a message from a Client, which it may process, or relay to another Server.
SOAP	W3C Simple Object Access Protocol Version 1.2. (http://www.w3.org/TR/soap12-part1/)
Standard	A standard is a document, established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.[73]
Standard Development Organization	Standards Development Organizations (SDOs) are organizations whose processes are accredited by ANSI. A SDO may also include non-ANSI accredited organizations such as W3C, OASIS, ISO, UN/CEFACT and IETF.
Support [Supported]	Means that the entity must have the capability as specified and required.

[69] http://www.atis.org/tg2k/ and search "Overhead Information" ATIS (Alliance for Telecommunications Industry Solutions http://www.atis.org/about.shtml
[70] CORE Phase I Glossary Definitions. www.caqh.org/pdf/COREPIGlossary.pdf
[71] CORE Phase I Glossary Definitions. http://www.caqh.org/pdf/COREPIGlossary.pdf
[72] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>
[73] http://isotc.iso.org/livelink/livelink/fetch/2000/2122/830949/3934883/3935096/07_gen_info/faq.html

Term or Concept	Definition
Submitter Authentication Standard C	Username-Password, described in Sub-section "Submitter Authentication Handling."
Submitter Authentication Standard D	X.509 Certificate based Authentication over SSL[74], described in Sub-section "Submitter Authentication Handling."
Synchronous	The application sending the request message waits for the response, which is returned on the same communications connection (i.e., synchronous request/reply). This message exchange pattern is used for most real time transactions.
Transport Layer Security (TLS)	Transport Layer Security (TLS)[75] and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that "provide communications security over the Internet". TLS and SSL encrypt the segments of network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP). TLS is an IETF standards track protocol, last updated in RFC 5246, and is based on the earlier SSL specifications developed by Netscape Corporation (http://tools.ietf.org/html/rfc5246).
WSDL	W3C Web Services Definition Language Version 1.1 (http://www.w3.org/TR/2001/NOTE-wsdl-20010315).

[74] Reference §3.1 for more information regarding the use of SSL and the optional use of TLS 1.0.
[75] http://en.wikipedia.org/wiki/Transport_Layer_Security

6.2 References

Note: These were used for Rule creation as well as to create the analysis artifacts as part of CORE Phase II Connectivity.

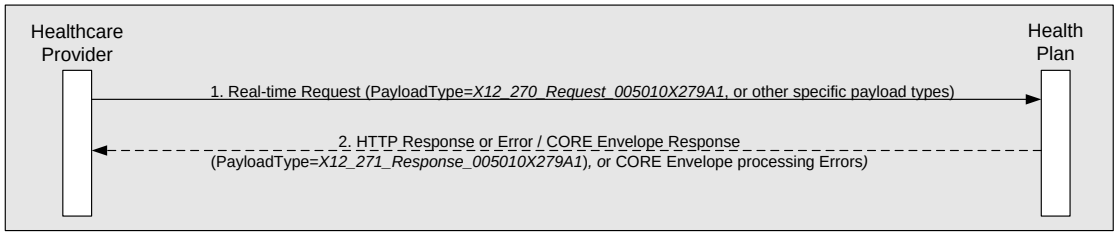
Author	Document Name	Location
CORE	Claim Status Rule Test Scenario	CORE Operating Rule 250
HL7 (Health Level 7)	HL7 Object Identifier (OID) Registry	http://www.hl7.org/oid/index.cfm
Internet Assigned Numbers Authority (IANA)	IANA Private Enterprise Number (PEN) aka "OID" Registration Page	http://www.iana.org/cgi-bin/enterprise.pl
Internet Engineering Task Force (IETF)	Key Words for use in RFCs to Indicate Requirement Levels	http://www.ietf.org/rfc/rfc2119.txt
Internet Engineering Task Force (IETF)	Uniform Resource Identifier (URI): Generic Syntax	http://www.gbiv.com/protocols/uri/rfc/rfc3986.html
Internet Engineering Task Force (IETF)	Hypertext Transfer Protocol – HTTP 1.1	http://tools.ietf.org/html/rfc2616.txt
Internet Engineering Task Force (IETF)	HTTP Authentication: Basic and Digest Access Authentication	http://tools.ietf.org/html/rfc2617.txt
Internet Engineering Task Force (IETF)	The MIME Multipart/Form-Data (RFC 2388)	http://www.ietf.org/rfc/rfc2388.txt
Internet Engineering Task Force (IETF)	TLS 1.1 Specification	http://tools.ietf.org/html/rfc4346.txt
Internet Engineering Task Force (IETF)	Universally Unique IDentifier (UUID) URN Namespace	ftp://ftp.rfc-editor.org/in-notes/rfc4122.txt
OASIS	Web Services Reliable Messaging Protocol 1.1 (WS-RM)	http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.html
OASIS	Web Service Security Core Specification 1.1	http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
OASIS	Web Service Security SOAP Message Security 1.1	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf
OASIS	Web Service Secure Conversation 1.3	http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html
OASIS	Universal Description, Discovery and Integration (UDDI) 1.0	http://www.oasis-open.org/committees/uddi-spec/doc/contribs.htm#uddiv1
OASIS	ebXML Message Service Specification v2.0	http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf
W3C (World Wide Web Consortium)	Extensible Mark-up Language (XML) 1.0 (Fourth Edition)	http://www.w3.org/TR/2006/REC-xml-20060816/
W3C (World Wide Web Consortium)	Namespaces in XML 1.0 (Second Edition)	http://www.w3.org/TR/2006/REC-xml-names-20060816
W3C (World Wide Web Consortium)	Canonical XML Version 1.0	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
W3C (World Wide Web Consortium)	XML Schema Part 1: Structures Second Edition	http://www.w3.org/TR/2004/REC-xmlschema-1-20041028
W3C (World Wide Web Consortium)	XML Schema Part 2: Datatypes Second Edition	http://www.w3.org/TR/2004/REC-xmlschema-2-20041028
W3C (World Wide Web Consortium)	XML Signature Syntax and Processing	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
W3C (World Wide Web Consortium)	XML Encryption Syntax and processing	http://www.w3.org/TR/2002/REC-xmlenc-core-20021210
W3C (World Wide Web Consortium)	Simple Object Access Protocol (SOAP) 1.2	http://www.w3.org/TR/soap12-part1/
W3C (World Wide Web Consortium)	SOAP Message Transmission Optimization Mechanism (MTOM)	http://www.w3.org/TR/2005/REC-soap12-mtom-20050125
W3C (World Wide Web Consortium)	Web Services Description Language (WSDL) 1.1	http://www.w3.org/TR/2001/NOTE-wsdl-20010315
Web Services Interoperability Organization	SOAP Basic Profile 1.1	http://www.ws-i.org/Profiles/BasicProfile-1.1-2006-04-10.html

6.3 Sequence Diagrams

The UML sequence diagrams below show interactions between a client (typically, a Health Care Provider) and a server (typically, a Health Plan). When the interactions include multiple requests/responses, each pair of requests and its corresponding (synchronous) response is shown encapsulated in a white rectangle. Each request followed by synchronous response (shown in a single white rectangle) is in a client-server connection that can be expected to be opened for a request and closed after the corresponding synchronous response is received. Subsequent requests/responses occur in new client-server connections. Servers are stateless and are not assumed to keep session information between connections, unless such information is sent as part of the requests (e.g., using 999 or TA1 payloads).

6.3.1 Real Time Interaction

The UML sequence diagram below shows a typical Real time Interaction between a Healthcare Provider and a Health Plan. The interactions are described in the diagram below.



The following describes the typical Real time interaction as shown in the above diagram.

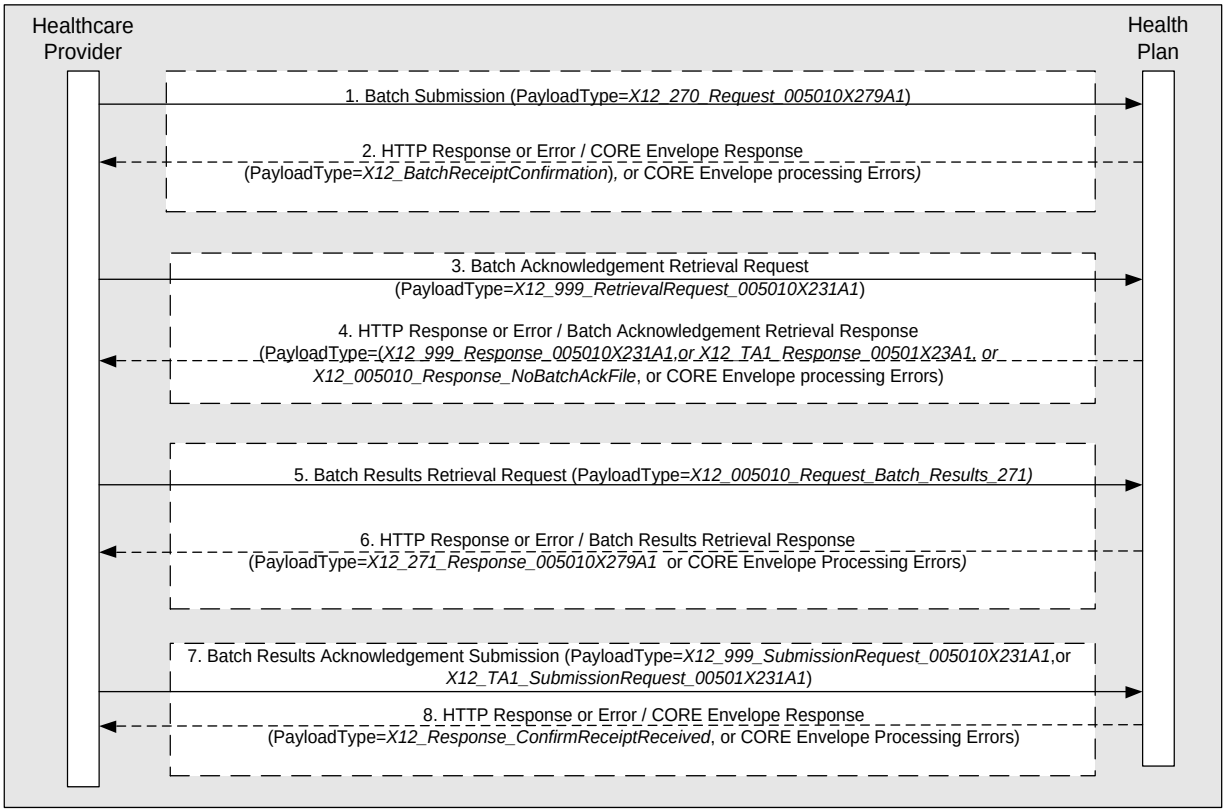
Message Sequence	Description	Reference to Section 4.4.3.1 Payload Type Table Transaction Name Column
1	Healthcare Provider submits a Real time request to the Health Plan, using payload type as X12_270_Request_005010X279A1, or one of the specific payload types (shown in section 4.4.3.1).	Health Care Eligibility Benefit Inquiry and Response
2	Health Plan responds (synchronously to request message 1) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (Payload type is X12_271_Response_005010X279A1, or error).	Health Care Eligibility Benefit Inquiry and Response

6.3.2 Batch Interaction

These sequence diagrams are non-normative examples of two types of Batch interactions. The Batch interactions can be conducted using specific payload types as shown in 6.3.2.1 or with Mixed Payload types as show in 6.3.2.2.

6.3.2.1 Batch Interaction for Specific Payload Types

The UML sequence diagram below shows a typical Batch Interaction between a Healthcare Provider and a Health Plan specifically for ASC X12 270/271 batch payloads (the same interaction applies to ASC X12 276/277 batch payloads).



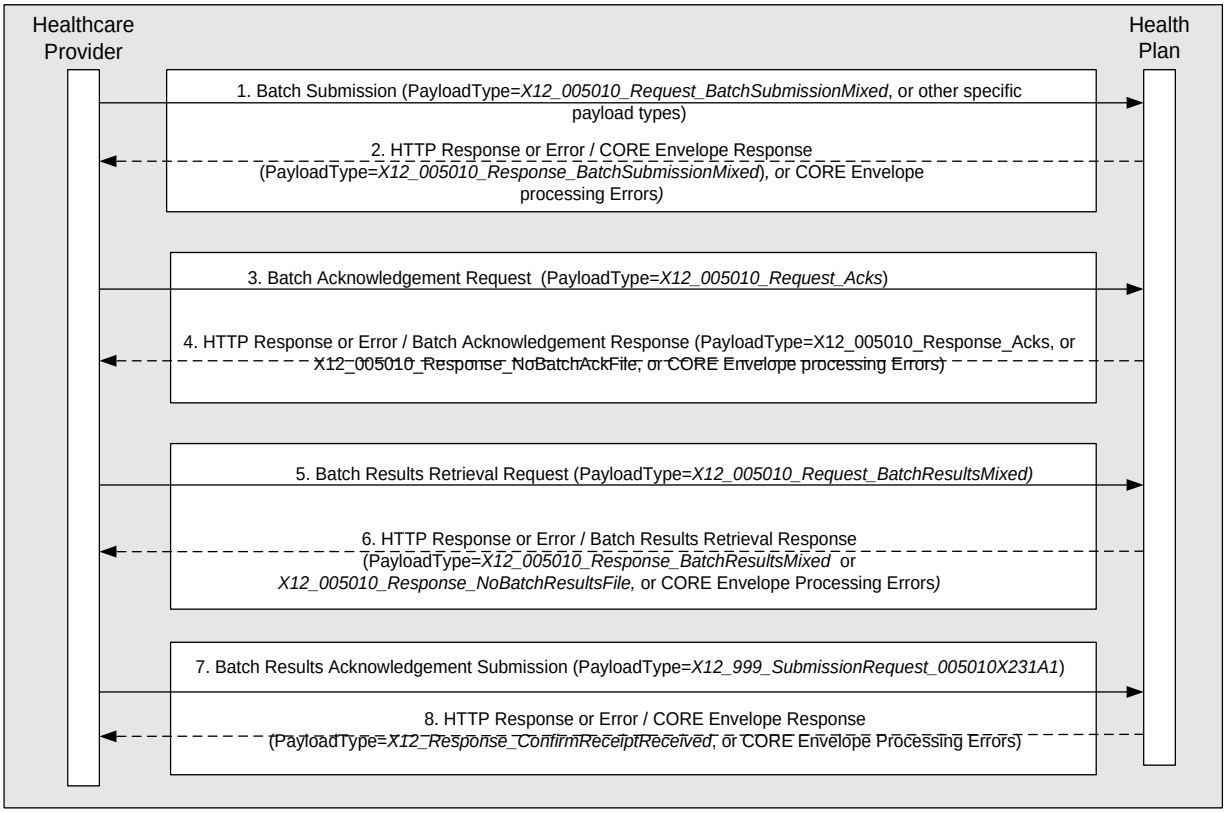
The following describes the Batch interaction as shown in the above diagram.

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
1	Healthcare Provider submits a Batch of requests to the Health Plan, using payload type as X12_270_Request_005010X279A1.	Health Care Eligibility Benefit Inquiry and Response
2	Health Plan responds (synchronously to request message 1) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch was received (e.g., payload type = X12_BatchReceiptConfirmation) and the CORE envelope was processed (with or without errors).	Health Care Eligibility Benefit Inquiry and Response
3	Healthcare Provider sends a Request to the Health Plan to solicit the acknowledgement (X12_999_RetrievalRequest_005010X231A1) for the Batch file	Implementation Acknowledgement

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
	that was just submitted.	Retrieval
4 I	Health Plan responds (synchronously to request message 3) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), with the X12_999_Response_005010X231A1 or an X12_TA1_Response_005010X231A1 acknowledgement. If no v5010 999 or TA1 is ready for pickup, Health Plan sends a CORE Envelope with payload type set to X12_005010_Response_NoBatchAckFile.	Implementation Acknowledgement Retrieval
5	Healthcare Provider sends a Request to the Health Plan to solicit the Results for the Batch file that was submitted in message sequence 1 using X12_005010_Request_Batch_Results_271.	Health Care Eligibility Benefit Inquiry and Response
6	Health Plan responds (synchronously to request message 5) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), with the payload type set to X12_271_Response_005010X279A1, and sends the result file as payload.	Health Care Eligibility Benefit Inquiry and Response
7	Healthcare Provider submits the acknowledgement (payload type X12_999_SubmissionRequest_005010X231A1, X12_TA1_SubmissionRequest_00501X231A1) to the Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Implementation Acknowledgement Submission (Request)
8	Health Plan responds (synchronously to request message 7) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch results acknowledgement was received (payload type = X12_Response_ConfirmReceiptReceived) and the CORE envelope was processed (with or without errors).	Implementation Acknowledgement Submission (Response)

6.3.2.2 Batch Interaction for Mixed Payload Types

The UML sequence diagram below shows a Mixed Payload Type Batch Interaction between a Healthcare Provider and a Health Plan.



The following describes the typical Mixed Batch interaction as shown in the above diagram.

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
1	Healthcare Provider submits a Batch of requests to the Health Plan, using payload type as BatchSubmissionMixed (e.g., payload type=X12_005010_Request_BatchSubmissionMixed), or one of the specific payload types (shown in section 4.4.3.2).	Batch Submission (mixed payload types)
2	Health Plan responds (synchronously to request message 1) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch was received (e.g., payload type = X12_005010_Response_BatchSubmissionMixed) and the CORE envelope was processed (with or without errors).	Batch Submission (mixed payload types)
3	Healthcare Provider sends a Request to the Health Plan to solicit the acknowledgement (ASC X12 v5010 999 or TA1 for the Batch file that was just submitted.	General Acknowledgements Pick Up

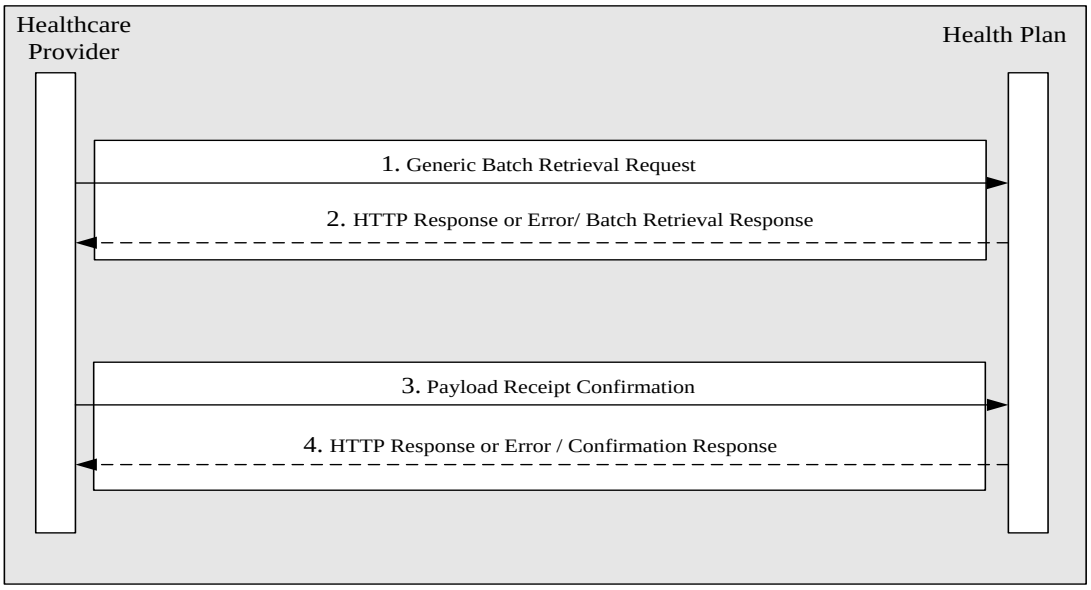
Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
4	Health Plan responds (synchronously to request message 3) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), with the ASC X12 v5010 999 or an X12_TA1 acknowledgement. If no v5010 999 or TA1 is ready for pickup, Health Plan sends a CORE Envelope with payload type set to X12_005010_Response_NoBatchAckFile, or X12_005010_Response_Acks.	No Acknowledgement File or General Acknowledgements Pickup
5	Healthcare Provider sends a Request to the Health Plan to solicit the Results for the Batch file that was submitted in message sequence 1.	Batch Results Retrieval (mixed payload types)
6	Health Plan responds (synchronously to request message 5) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), with the payload type set to X12_005010_Response_BatchResultsMixed, and sends the result file as payload. If no results file is ready for pickup, Health Plan sends a CORE Envelope with payload type set to X12_005010_Response_NoBatchResultsFile.	• Batch Results Retrieval (mixed payload types) • No Acknowledgement File
7	Healthcare Provider submits the acknowledgement (payload type X12_999_SubmissionRequest_005010X231A1 or X12_TA1_SubmissionRequest_005010X231A1) to the Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Implementation Acknowledgement Submission
8	Health Plan responds (synchronously to request message 7) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch results acknowledgement was received (payload type = X12_Response_ConfirmReceiptReceived) and the CORE envelope was processed (with or without errors).	Implementation Acknowledgement Submission

6.3.3 Generic Batch Retrieval Request and Receipt Confirmation

The UML sequence diagram below shows a Generic Batch Retrieval Request and Receipt Confirmation interaction between a Healthcare Provider and a Health Plan.

If this interaction is used for a Healthcare Claim Acknowledgement, there is a pre-condition in this interaction. In this case, the Healthcare Provider must have previously submitted a claim to the Health Plan and the Healthcare Provider is now requesting information about that claim.

The message interactions are described in the diagram below.



The following describes the typical Batch Retrieval interaction as shown in the above diagram.

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
1	Healthcare Provider submits a Generic Batch Retrieval Request to the Health Plan, using a valid PayloadType from the table in section 4.4.3.2.	• Health Care Claim Acknowledgement • Health Care Claim Payment/Advice • Health Care Claim Pending Status Information
2	Health Plan responds synchronously in Real time with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch was received and the CORE envelope was processed without errors	• Health Care Claim Acknowledgement • Health Care Claim Payment/Advice • Health Care Claim Pending Status Information
3[76]	Health Care Provider sends to Health Plan a confirmation that it received the payload sent in step 2.	Payload Receipt Confirmation

[76] Since step 3 is a new connection (session) from the Provider to the Plan, for there to be an association of the Receipt Confirmation sent in this connection with the previously received retrieval response, this confirmation needs to be a 999 or a TA1.

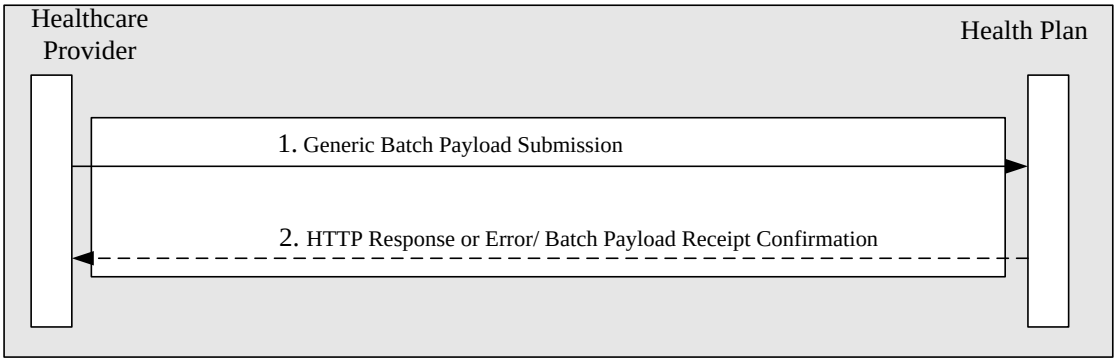
Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
4	Health Plan responds (synchronously to request message 3) to the request either with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response, or CORE Envelope Error.	Payload Receipt Confirmation

6.3.4 Generic Batch Submission with Batch Payload and Synchronous Payload Receipt Confirmation

The UML sequence diagram below shows a Generic Batch Payload Submission and Synchronous Payload Receipt Confirmation interaction between a Healthcare Provider and a Health Plan (Note: The submission of a Generic Batch may be performed by a stakeholder other than a Healthcare Provider, e.g., a Health Plan Sponsor.)

This interaction allows us to specify only the steps necessary for a Client (typically, a Healthcare Provider) to perform a Batch Payload submission to a Server (typically, a Health Plan) and receive the corresponding synchronous receipt confirmation. In terms of the actual request and response, the Generic Batch Submission Interaction also happens to be a subset of entire Batch Interaction (§6.3.2). The part of the WSDL (for SOAP envelope) that has been extended to describe the Generic Batch Submission Interaction shows how that interaction re-uses the existing Batch Submission request/response messages, for which examples are provided in section 4. For this reason, footnotes have been provided where the existing Batch Submission examples also serve as examples for the Generic Batch Submission message interaction.

The message interactions are described in the diagram below.



The following describes the typical Generic Batch Submission interaction as shown in the above diagram.

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
1	Healthcare Provider submits a Batch Payload to a Health Plan using a valid PayloadType from the table in §4.4.3.	• Health Care Claim Request for Additional Information • Request for Information in Support of a Disability Claim • Health Care Claim: Institutional • Health Care Claim: Professional • Health Care Claim: Dental • Payroll Deducted and Other

Message Sequence	Description	Reference to Section 4.4.3.2 Payload Type Table Transaction Name Column
		Group Premium Payment for Insurance Products • Benefit Enrollment and Maintenance • Health Care Benefit Coordination Verification • Health Care Predetermination – Professional • Health Care Predetermination – Institutional • Doctors First Report of Injury • Health Care Service: Data Reporting
2	Health Plan responds synchronously in Real time with an HTTP level error, or an HTTP successful response accompanied by a CORE envelope level response (or error), indicating that the Batch was received and the CORE envelope was processed without errors.	• Health Care Claim: Institutional • Health Care Claim: Professional • Health Care Claim: Dental • Payroll Deducted and Other Group Premium Payment for Insurance Products • Benefit Enrollment and Maintenance • Health Care Benefit Coordination Verification • Health Care Predetermination – Professional • Health Care Predetermination – Institutional • Doctors First Report of Injury • Health Care Service: Data Reporting

