

MEDICARE FEE-FOR-SERVICE

Standard Companion Guide Trading Partner Information

Instructions Related to Transactions Based on
ASC X12 Implementation Guides, Version 005010

Companion Guide Version Number: 5.0
Revised: August 2018

PREFACE

Companion Guides (CG) may contain two types of data, instructions for electronic communications with the publishing entity (Trading Partner Information) and supplemental information for creating transactions for the publishing entity while ensuring compliance with the associated ASC X12 Implementation Guide (IG) (Transaction Instructions). Either the Trading Partner Information component or the Transaction Instruction component must be included in every CG. The components may be published as separate documents or as a single document.

The Trading Partner Information component is included in the CG when the publishing entity wants to convey the information needed to commence and maintain communication exchange.

The Transaction Instruction component is included in the CG when the publishing entity wants to clarify the IG instructions for submission of specific electronic transactions. The Transaction Instruction component content is limited by the ASC X12 copyrights and Fair Use statement.

Table of Contents

PREFACE.....	2
I. Trading Partner Information Introduction.....	5
1.1 Purpose	5
1.2 Scope	5
1.3 Overview	6
1.4 References	7
1.5 Additional Information	7
II. Getting Started	8
2.1 Working Together	8
2.2 Trading Partner Registration	8
2.3 Trading Partner Testing and Certification Process	11
III. Testing and Certification Requirements	13
3.1 Testing Requirements	13
3.2 Certification Requirements.....	13
IV. Connectivity/Communications	14
4.1 Process Flows for Batch Submissions.....	14
4.2 Transmission Administrative Procedures.....	15
4.3 Re-transmission Procedures	16
4.4 Best Practices for Transmission.....	17
4.5 Communication Protocols	17
4.6 Security Protocols	17
V. Contact information	19
5.1 EDI Customer Service	19
5.2 EDI Technical Assistance	19
5.3 Provider Services	19
5.4 Applicable Websites/Email.....	19
VI. Control Segments / Envelopes	20
6.1 ISA-IEA.....	22
6.2 GS-GE.....	23
6.3 ST-SE.....	23
VII. Acknowledgements and Reports	24
7.1 ASC X12 Acknowledgments	24
7.2 Report Inventory.....	24

VIII. Additional Trading Partner Information.....26

8.1 Implementation Checklist 26

8.2 Transmission Examples: Control Segment Examples..... 26

8.3 Trading Partner Agreement..... 27

8.4 Frequently Asked Questions 28

8.5 Other Resources 28

IX. Trading Partner Information Change Summary.....29

X. Appendices.....30

I. Trading Partner Information Introduction

1.1 Purpose

This document is intended to provide information from the author of this guide to trading partners to give them the information they need to exchange electronic data interchange (EDI) data with the author. This includes information about registration, testing, support, and specific information about control record setup.

An EDI Trading Partner is defined as any Medicare customer (e.g., provider/supplier, billing service, clearinghouse, or software vendor) that transmits to, or receives electronic data from, Medicare. Medicare's EDI transaction system supports transactions adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as additional supporting transactions as described in this guide.

Medicare Fee-for-Service (FFS) is publishing this Companion Guide to clarify, supplement and further define specific data content requirements to be used in conjunction with, and not in place of, the ASCX12N TR3s for all transactions mandated by HIPAA and/or adopted by Medicare FFS for EDI.

This Companion Guide provides communication, connectivity and transaction specific information to Medicare FFS trading partners and serves as the authoritative source for Medicare FFS specific EDI protocols.

Additional information on Medicare FFS EDI practices are referenced in the [Centers for Medicare & Medicaid Services \(CMS\) Internet-Only Manual \(IOM\) Publication 100-04, Medicare Claims Processing Manual, Chapter 24, "General EDI and EDI Support Requirements, Electronic Claims, and Mandatory Electronic Filing of Medicare Claims"](#) (674 KB)

1.2 Scope

EDI addresses how providers /suppliers, or their business associates, exchange professional and institutional claims, claim acknowledgments, claim remittance advice, claim status inquiry and response, and eligibility inquiry and response electronic transactions with Medicare. This guide also applies to the above referenced transactions that are being exchanged with Medicare by third parties, such as clearinghouses, billing services or network service vendors. Below is a listing of transactions required by Medicare FFS:

Transactions	Version
270/271 Health Care Eligibility Benefit Inquiry and Response	005010X279A1
837 Health Care Claim: Professional	005010X222A1
837 Health Care Claim: Institutional	005010X223A2
999 Implementation Acknowledgment for Health Care Insurance	005010X231A1
835 Health Care Claim Payment/Advice	005010X221A1
276/277 Status Inquiry and Response	005010X212
277CA Claim Acknowledgement	005010X214
National Council for Prescription Drug Programs (NCPDP) Version D.0 of the Telecom Standard	D.0 April 2009

This Companion Guide provides technical and connectivity specification for the following above listed transactions:

- 837 Health Care Claim : Institutional
- 837 Health Care Claim : Professional
- 835 Health Care Claim : Payment Advice
- 276/277 Status Inquiry and Response

Technical specifications for the 999 Implementation Acknowledgement for Health Care Insurance and 277CA Claim Acknowledgement are subsumed under the technical specifications for the 837 Institutional and Professional Claim transaction.

The 270/271 Health Care Eligibility Benefit Inquiry and Response has its own companion guide that can be found at <https://www.cms.gov/HETSHelp/>.

NCPDP Version D.0 also has its own companion guide that can be found at <https://www.NGSCEDI.com/>

1.3 Overview

This Companion Guide includes information needed to commence and maintain communication exchange with Medicare. In addition, this Companion Guide has been written to assist you in designing and implementing transaction standards to meet Medicare's processing standards. This information is organized in the sections listed below:

- **Getting Started:** This section includes information related to system operating hours, provider data services, and audit procedures. Information concerning Trading Partner registration and the Trading Partner testing process is also included in this section.
- **Testing and Certification Requirements:** This section includes detailed transaction testing information as well as certification requirements needed to complete transaction testing with Medicare.
- **Connectivity/Communications:** This section includes information on Medicare's transmission procedures as well as communication and security protocols.
- **Contact Information:** This section includes EDI customer service, EDI technical assistance, provider services and applicable Websites.
- **Control Segments/Envelopes:** This section contains information needed to create the ISA/IEA, GS/GE and ST/SE control segments for transactions to be submitted to Medicare.
- **Acknowledgements and Reports:** This section contains information on all transaction acknowledgments sent by Medicare and report inventory.
- **Additional Trading Partner Information:** This section contains information related to implementation checklist, transmission examples, Trading Partner Agreements and other resources.
- **Trading Partner Information Change Summary:** This section describes the differences between the current Companion Guide and the previous Companion Guide(s).

1.4 References

The following websites provide information for where to obtain documentation for Medicare adopted EDI transactions, code sets and telecommunications.

Resource	Web Address
ASC X12 TR3 Implementation Guides	http://store.X12.org
Washington Publishing Company Health Care Code Sets	http://www.wpc-edi.com/
CMS instructs for the Affordable Care Act - Operating Rules - Requirements for Phase II and Phase III Compliance for Batch Processing	MLN Matters MM9358
CAQH CORE Operating Rules II and III	http://www.caqh.org/core/operating-rules

1.5 Additional Information

The websites listed below provide additional resources during the transition year for HIPAA version 5010 implementation.

Resource	Web Address
Central Version 005010 and D.0 web page on the CMS website	https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Versions5010andD0/index.html
Educational Resources (including MLN articles, fact sheets, readiness checklists, brochures, quick reference charts and guides, and transcripts from national provider calls)	https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Versions5010andD0/40_Educational_Resources.html
Frequently Asked Questions	https://questions.cms.gov/faq.php?isDept=0&search=5010&searchType=keyword&submitSearch=1&id=5005
Responses to Technical Comments	https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AdoptedStandardsandOperatingRules.html
To request changes to HIPAA adopted standards	http://www.hipaa-dsmo.org/
Medicare FFS EDI Operations : Provider's operational information for FI and electronic transaction standards	https://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/EDISupport.html

II. Getting Started

2.1 Working Together

National Government Services (NGS) is dedicated to providing several communication channels to ensure communication remains constant and efficient. NGS has several options in an effort to assist the community with their electronic data exchange needs. By using any of these methods NGS is focused on supplying the Trading Partner community with a variety of support tools.

The EDI Help Desk is established for the first point of contact for basic information and troubleshooting. The help desk is available to support most EDI questions/incidents while at the same time being structured to triage each incident if more advanced research is needed. An EDI email is also accessible as a method of communicating with NGS. The email account is monitored by knowledgeable staff ready to assist you. When communicating via email, please exclude any Protected Health Information (PHI) to ensure security is maintained. In addition to the NGS EDI Help Desk and email access, feel free to communicate via alternative methods (see section 5 for contact information).

NGS also has several external communication components in place to reach out to the trading partner community. NGS posts all critical updates, system issues and EDI specific billing material on their website at <https://www.NGSMedicare.com>. All Trading Partners are encouraged to visit this page to ensure familiarity with the content of the site. NGS also distributes EDI pertinent information in the form of a monthly bulletin. The monthly bulletin is posted to the NGS website every month. In addition to the website, a distribution list has been established in order to broadcast urgent messages. Please register for the NGS email distribution list at <https://www.NGSMedicare.com> by selecting **Subscribe to Email Updates** to register with the appropriate line of business

Specific information about the above-mentioned items can be found in the following sections.

2.2 Trading Partner Registration

An EDI Trading Partner is any entity (provider, billing service, software vendor, employer group, financial institution, etc.) that will transmit electronic data to or receives electronic data from another entity.

Medicare FFS and NGS support many different types of customers for EDI. To ensure proper registration it is important to understand the terminology associated with each customer type.

- **Submitter:** The entity that owns the submitter ID associated with the healthcare data being submitted. It is most likely the provider, hospital, clinic, supplier, etc., but could also be a third party submitting on behalf of one of these entities. However, a submitter must be directly linked to each billing provider (NPI). Often the terms submitter and trading partner are used interchangeably because a **Trading Partner** is defined as the entity engaged in the exchange or transmission of electronic transactions. Thus, the entity that is submitting electronic transactions to NGS is a Medicare FFS trading partner.
- **Provider/Supplier:** The entity that renders services to beneficiaries and submits health care claims to Medicare.

- **Vendor:** An entity that provides hardware, software and/or ongoing technical support for covered entities. In EDI, a vendor can be classified as a software vendor, billing or network service vendor or clearinghouse.
- **Software Vendor:** An entity that creates software used by billing services, clearinghouses and providers/suppliers to conduct the exchange of electronic transactions with Medicare FFS.
- **Billing Service:** A third party that prepares and/or submits claims for a provider/supplier.
- **Clearinghouse:** A third party that submits and/or exchanges electronic transactions (claims, claim status or eligibility inquiries, remittance advice, etc.) on behalf of a provider/supplier.
- **Network Service Vendor (NSV):** A third party that provides connectivity between a provider, supplier, clearing house or billing service and NGS.
- **Certificate Authority (CA):** A third party that provides X.509 Digital Certificates for authentication for connectivity to the NGS EDI Internet Gateway.

Providers are required to submit all claims electronically unless they have submitted and been approved for an Administrative Simplification Compliance Act (ASCA) waiver. Information regarding qualifying and filing an ASCA waiver is posted at <https://www.NGSMedicare.com> under the **Claims & Appeals** section.

Note: Medicare Part B can only accept one prior payer; any Part B claim with more than one prior payer must be submitted on paper. As a reminder, an ASCA waiver must be on file prior to submitting paper claims

Medicare requires all trading partners to complete EDI registration to obtain access to the EDI sFTP and EDI Internet Gateways (sFTP & Internet Gateways). All providers must sign an EDI Enrollment form. The EDI Enrollment form designates the Medicare contractor and/or CEDI as the entity they agree to engage in for EDI and ensures agreement between parties to implement standard policies and practices to ensure the security and integrity of information exchanged. The forms can be accessed at <https://www.NGSMedicare.com>. Entities processing paper do not need to enroll with EDI.

To register with NGS EDI, providers must complete the following registration forms:

- The EDI Enrollment Agreement which indicates providers' acceptance to comply with CMS instructions for use of electronic transactions,
- The EDI Registration Form to request a submitter identifier (ID).

If the provider will be using a clearinghouse or other third-party billing service, the provider must also submit an EDI Registration Form. A clearinghouse or other third-party billing service may register for a submitter ID by completing the EDI Registration Form. Third party submitters will not be issued a submitter ID unless a provider has submitted an EDI Registration form authorizing the third party to perform EDI transactions on their behalf.

The EDI registration forms are submitted online via the NGS website at <https://www.NGSMedicare.com>, select **Claims & Appeals > EDI Enrollment** option.

Section 4 of this guide contains detailed information needed to complete the EDI registration regarding NGS EDI connectivity options.

Under HIPAA, EDI applies to all covered entities transmitting the following administrative transactions: 837I and 837P, 835, 270/271, 276/277 and NCPDP. As of 1/1/2011, Medicare contractors and CEDI use the TA1, 999 and 277CA error handling transactions.

Medicare requires that we furnish new providers/suppliers that request Medicare claim privileges information on EDI. Additionally, Medicare requires us to assess the capability of entities to submit data electronically, establish their qualifications (see test requirements in Section 3.0 below), and enroll and assign submitter EDI identification numbers to those approved to use EDI. The EDI enrollment process for the Medicare beneficiary inquiry system (HIPAA Eligibility Transaction System [HETS] 270/271) is currently a separate process. Information on the EDI enrollment process for HETS can be found on the CMS HETS Help website at <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html?redirect=/HETSHelp>.

A provider must obtain an NPI and furnish that NPI to NGS prior to completion of an initial EDI Enrollment Agreement and issuance of an initial EDI number and password by that contractor. This EDI number and password is required to login to the NGS sFTP Gateway as well as for identification of the submitter within the HIPAA transactions.

NGS is required to verify that NPI submitted on the Enrollment form against the NPI Crosswalk. If the NPI is not verified on the NPI Crosswalk, the EDI Enrollment Agreement is denied and the provider is encouraged to contact NGS Provider Enrollment department to resolve the issue. Once the NPI is properly verified, the provider can resubmit an EDI Enrollment Agreement.

A provider's EDI number and password serve as a provider's electronic signature and the provider would be liable if any entity with which the provider improperly shared the ID and password performed an illegal action while using that ID and password. A provider's EDI access number and password are not part of the capital property of the provider's operation, and may not be given to a new owner of the provider's operation. A new owner must obtain their own EDI access number and password. This same requirement applies to the Digital Certificates required for NGS Internet Gateway access (see Section 4). A new owner would be required to obtain a new Digital Certificate to link to the new EDI number.

If providers elect to submit/receive transactions electronically using a third party such as a billing agent, a clearinghouse or network service vendor, they are required to have an agreement signed by that third party. The third party must agree to meet the same Medicare security and privacy requirements that apply to the provider in regard to viewing or use of Medicare beneficiary data. These agreements are not to be submitted to Medicare, but are to be retained by the providers. Providers will notify NGS which third party agents they will be using on their EDI Registration form.

Third parties are required to register with NGS by completing the EDI Registration form. This will insure that their connectivity is completed properly; however, a separate enrollment may be required for enrollment in mailing lists to receive all publications and email notifications.

This agreement is available for online submission via the NGS website at <https://www.NGSMedicare.com>, under **Claims & Appeals > EDI Enrollment**.

Providers must also be informed that they are not permitted to share their personal EDI access number and password with any billing agent, clearinghouse/network service vendor. Providers must also not share their personal EDI access number with anyone on their own staff who

does not need to see the data for completion of a valid electronic claim, to process a remittance advice for a claim, to verify beneficiary eligibility, or to determine the status of a claim. No other non-staff individuals or entities may be permitted to use a provider's EDI number and password to access Medicare systems.

Clearinghouse and other third party representatives must obtain and use their own unique EDI access number and password from NGS. For a complete reference to security requirements see Section 4.6 and refer to the Appendix A CMSR High Impact Level Data document located on the CMS website at <https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS1248023.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending>

Trading Partners who wish to use the Internet Gateway for batch file transfer activity for the 276/277 and 835 Transactions will continue to use the assigned EDI Number as the Submitter Identifier in the HIPPA transactions.

See Section 4.2 for more information on accessing the NGS Internet Gateway.

See Section 6 for detailed instructions for populating the Submitter Identifier in the HIPPA transactions.

FISS DDE Enrollment:

Part A providers that need access to the Fiscal Intermediary Standard System (FISS) Direct Data Entry (DDE) application may request user IDs using the Part A Logon Request Form. A provider must have an EDI Enrollment Form on file and have a connection to the Virtual Data Center (VDC) through one of the NSVs.

The Part A Logon Request Form is available for online submission via the NGS website at <https://www.NGSMedicare.com> under the **Claims & Appeals tab**, then select **EDI Enrollment**.

2.3 Trading Partner Testing and Certification Process

New NGS submitters are required to test with NGS. The exception is new submitters who are using an approved vendor software package or the PC-ACE free billing software.

Claims Testing

Testing is available to all submitters 24/7.

Test 837 claim files should be limited to 25-100 claims. (ISA15 Test/Prod Indicator submitted with a 'T').

The TRN report and acknowledgement transactions TA1 and 999 will be available within minutes.

The 277 Claims Acknowledgment (277CA) will follow within 2 hours of the TA1 and 999 transactions. The acknowledgement transactions will require translation to a 'human readable' or text format.

See Section 7 for more detail on Reports and Acknowledgments

Test claims will not be sent to the claims systems.

Production Criteria for 837 Claims:

Level I syntax compliance – 100%

- 999 Acknowledgement status is 'Accepted'
- Level II Medicare situational and business edit compliance – 95%
- 277 Claims Acknowledgement indicates 95% claim acceptance
- Trading Partners will be notified with approval for production for 837 claims submission

276/277 Claim Status Inquiry & Response Transaction Testing

- 276/277 testing is limited to Level 1 syntax compliance validation of the 276 transaction; a test 277 transaction will not be returned.
- A 276 Claim Status Inquiry Transaction must be submitted with a production, 'P' indicator in the Test/Prod Indicator data element, ISA15, to generate a 277 Claims Status Response file.

835 Electronic Remittance Advice Testing

- 835 testing is supported in production
- An 835 Electronic Remittance Advice will be generated in production along with the Standard Paper Remittance for comparison.
 - For Part A, the paper remittance is generated for 31 day
 - For Part B, the paper remittance is generated for 45 days

Testing of the approved transactions for the Internet Gateway, 276/277 and 835, is limited to the file transfer functionality. A Trading Partner must have an X.509 Digital Certificate on file with NGS. Trading Partners will transmit the Certificate information via the NGS Traditional Gateway. (See Section 4.2 for details)

- A response indicating the receipt and validity of the Certificate data will be returned. Trading Partners can begin to submit 276 files or download 835 ERA files once the 'good' response has been received.
- A 277 Claims Status Response file will not be generated for submitted 276 Claims Status Inquiries test files.

The Internet Gateway does not allow the submission of 837 Claim files at this time.

III. Testing and Certification Requirements

3.1 Testing Requirements

All claim submitters must produce accurate electronic test claims before being allowed to submit claim transactions in production. All submitters must send a test file containing at least 25 claims, which are representative of their practice or services. The number of claims could be increased or decreased, on a case by case basis, to ensure adequate testing of any given submitter. Test claims are subject to standard syntax and IG semantic data edits; documentation will be provided when this process detects errors.

- Standard syntax testing validates the programming of the incoming file and includes file layout, record sequencing, balancing, alpha-numeric/numeric/date file conventions, field values, and relational edits. Test files must pass 100 percent of the Standard syntax edits before production is approved.
- IG Semantic Data testing validates data required for claims processing, e.g., procedure/diagnosis codes, modifiers. A submitter must demonstrate, at a minimum, a 95 percent accuracy rate in data testing before production is approved where, in the judgment of NGS, the vendor/submitter will make the necessary correction(s) prior to submitting a production file. The minimum 95 percent accuracy rate includes the IG and Medicare business front-end edits.

Many claim submitters use the same software, or the same clearinghouse to submit their electronic claims to Medicare.

When appropriate, NGS will test and approve software vendor products for 5010 compliance with NGS. As vendors roll the 5010 compliant software to their clients, NGS will not require each of the clients (submitters) to test with NGS. NGS will work with each vendor as the software is transitioned to their clients (submitters) to move to 5010 in production mode.

Providers/suppliers who submit transactions directly to more than one A/B MAC, HHH-A and/or CEDI, and billing services and clearinghouses, must contact each A/B MAC, HHH-A and/or CEDI with whom they exchange EDI transactions to inquire about the need for supplemental testing whenever they plan to begin to use an additional EDI transaction, different or significantly modified software for submission of a previously used EDI transaction, or before a billing agent or clearinghouse begins to submit transactions on behalf of an additional provider. The individual A/B MAC, HHH-A and/or CEDI may need to retest at that time to re-establish compatibility and accuracy, particularly if there will also be a change in the telecommunication connection to be used.

Billing services and clearinghouses are not permitted to begin to submit or receive EDI transactions on behalf of a provider prior to submission of written authorization by the provider that the billing agent or clearinghouse has been authorized to handle those transactions on the provider's behalf. See Section 2.2 for further information on EDI enrollment.

3.2 Certification Requirements

Medicare FFS does not certify providers; however, NGS does certify vendors, clearinghouses, and billing services in the form of testing with them and maintaining an approved vendor list can be accessed online at <https://www.NGSMedicare.com>, select the **Claims & Appeals** tab, > **EDI Enrollment**.

IV. Connectivity/Communications

NGS facilitates the batch transmission of HIPAA and non HIPAA transactions of inbound and outbound files through its sFTP and Internet Gateways.

4.1 Process Flows for Batch Submissions

Process flows for batch submissions of the HIPAA Transactions Sets can be found in the front matter of the applicable TR3 (Implementation Guide).

NGS supports two EDI Gateways. Requirements for telecommunications for each Gateway are as follows:

sFTP Gateway

All submitters (providers and third-parties) must contract with a NGS NSV for connectivity to the sFTP Gateway. The list of approved NGS NSVs is available on the NGS website at <https://www.NGSMedicare.com>, under the **Claims & Appeals** tab, select the **EDI Enrollment** option then select the link for **Network Service Vendors**.

Internet Gateway

In addition to the sFTP Gateway solution, Trading Partners have the option to send/receive batch 276 Claim Status Inquiry transactions, 277 Response Transactions and receive 835 transactions via a NGS Internet EDI Gateway. This Internet solution has been developed to be compliant with CAQH/CORE Phase I, II and Phase III Batch and Telecommunications Operating Rules, excluding real time. The TA1 and 999 Transactions will also be available for download in response to 276 transactions.

Note: The Internet Gateway does not support batch file transfer of Medicare 837 Institutional or Professional claims at this time.

Trading Partners choosing to use the Internet Gateway for 276/277 file transfer and/or 835 ERA access will continue to have the capability to access the sFTP Gateway for batch file transfer activities for these transactions as well as for submission of their 837 claim file submissions. No additional EDI Enrollment forms are necessary for access to the NGS Internet Gateway.

Requirements for Trading Partners who wish to facilitate file transfer of the 276/277 Claim Status Inquiry and Claim Status Response and 835 ERA transactions over the Internet Gateway:

- Must support HTTP/S V1.1 transport over the Internet Gateway.
- Must support HTTP v1.1+ Message Envelope Standards and Message Exchanges:
 - {Hypertext Transfer Protocol & Multipurpose Internet Mail Extensions (HTTP+MIME) or
 - Simple Object Access Protocol & Web Service Definition Language (SOAP+WSDL) Message}.
 - Samples of HTTP+MIME and SOAP+WSDL Messaging Standards can be found in the CAQH CORE 270 Connectivity Operating Rules v2.2.0: <http://www.cagh.org/sites/default/files/core/phase-ii/policy-rules/270-v5010.pdf>

- Within the HTTP+MIME and SOAP+WSDL envelopes the Sender and Receiver IDs must be populated as follows:
 - Sender ID = NGS Assigned Trading Partner ID
 - Receiver ID = NGSEDI
- In the Outbound transactions, NGS will populate the Sender ID with NGSEDI and the NGS Assigned Trading Partner ID as the Receiver ID.
- Obtain x509 certificate for authentication purposes from the NGS preferred x.509 Certificate Vendors list. See Section 4.2 for sending certificate information to NGS.
- URL for HTTP:MIME Protocol:
<https://www.edi.ngsmedicare.com/CoreBatchGateway/TransactionSocketServlet>
- URL for SOAP/WSDL Protocol:
<https://www.edi.ngsmedicare.com/CoreBatchGateway/soap/coreservice?wsdl>

4.2 Transmission Administrative Procedures

NGS sFTP Gateway is accessed through a NGS approved NSV. NGS requires use of the sFTP protocol for file transfer.

A list of the approved NGS NSVs, can be found on the NGS website at <https://www.NGSMedicare.com>. Select the **Claims & Appeals tab, > EDI Enrollment > Network Service Vendors**.

Access to the NGS Internet Gateway requires the trading partner to share their X.509 digital certificate information with NGS for authentication purposes.

- Trading Partners will submit the X.509 file provided by the Certificate Authority to the NGS sFTP Gateway.
- Trading Partners will use the Submitter ID and password assigned for access to the sFTP Gateway to transfer the X.509 digital certificate file.
- NGS will validate the Certificate information and respond with the results of the validation via the TRN report.
 - Certificates must be obtained from the NGS approved Certificate Authority, DigiCert;
 - Certificates cannot be valid for longer than three (3) years;
 - Only one Certificate is allowed per Trading Partner (Submitter) ID;
 - A Trading Partner with multiple Submitter IDs, must provide a Certificate for each Submitter ID.
 - Certificates cannot be transferred from one Trading Partner to another
- The status of the transmission of the Certificate file will be communicated via the TRN report. If the file transfer is successful, a TRN Report will be generated indicating that no errors were identified. When the file transfer is unsuccessful, the following messages that may be returned are:

TRNACK when a Certificate has incomplete or missing certificate information

Error number = 101 Severity = 1

Incomplete or missing certificate information – Serial Number

Error number = 101 Severity = 1
 Incomplete or missing certificate information – Issuer DN

Error number = 101 Severity = 1
 Incomplete or missing certificate information – Subject DN

Error number = 101 Severity = 1
 Incomplete or missing certificate information – Start Date

Error number = 101 Severity = 1
 Incomplete or missing certificate information – End Date

TRNACK when a Certificate has already been loaded to current Org

Error number = 201 Severity = 1
 Duplicate - Certificate already on file for this Trading Partner

TRNACK when a Certificate has already been assigned to a different Org

Error number = 301 Severity = 1
 Certificate linked to another Trading Partner

TRNACK when a Certificate is expired

Error number = 401 Severity = 1
 Certificate Authority not approved - PKIX path validation failed:
 java.security.cert.CertPathValidatorException: timestamp check failed

TRNACK when a Certificate Authority is not approved

Error number = 401 Severity = 1
 Certificate Authority not approved – {message}

TRNACK when a Certificate is valid for more than 3 years

Error number = 501 Severity = 1
 Validity period > 3 years

TRNACK when a Certificate is invalid for an exception. This error may occur instead of the “101” errors.

Error number = 602 Severity = 1
 Certificate exception {message}

TRNACK when a Certificate is invalid, not properly formatted

Error number = 602 Severity = 1
 Fail to parse input stream

Note: TRN reports will be generated for 276 Claims Status Inquiry files sent via the NGS Internet Gateway; however, they will not be available for retrieval via the Internet Gateway. TRN Reports generated for 276 files submitted via either NGS Gateway will be available for retrieval via the NGS sFTP Gateway only.

4.3 Re-transmission Procedures

Submitters should not retransmit any file that has successfully passed EDI front-end editing without specific instruction from NGS.

Submitters may retransmit any file that has failed front-end editing, once the file has been corrected.

4.4 Best Practices for Transmission

File transfer for all HIPAA transactions is available 24/7. The following identify best practices and service levels for transaction processing.

- Do not run scripts that will continually log your Trading Partner ID into the EDI gateway checking for reports to download
- TRN, TA1 and 999 acknowledgements are available with a few minutes of sending the 837 claim file to NGS
- 277CA is available within two hours
- 835 remittances are available Tuesday – Saturday by noon
- 837 Claim files received by 5:00 p.m. ET will receive the same day receipt date. Claim files received after 5:00 p.m. ET will receive the receipt date of the next business day.
 - Examples:
 - Claim files received on a Monday after 5:00 p.m. will receive a receipt date of the next business day (Tuesday).
 - Claim files received after 5:00 pm on a Friday will receive the receipt date of the following Monday.
 - If the next business day is a holiday, the receipt date will be the next business day following the holiday.
- 276 transactions submitted by 9:00 p.m. ET through either the sFTP Gateway or the Internet Gateway will receive a 277 Claim Status Response by 7:00 a.m. ET the next business day.

4.5 Communication Protocols

NGS supports Secured FTP (sFTP) protocol for all EDI file transfer activity through the NGS sFTP Gateway. Connectivity to this gateway is obtained through an NGS-approved NSV.

The NGS Internet Gateway requires the following protocols:

- HTTP/S V1.1
- HTTP/MIME; or
- SOAP/WSDL

4.6 Security Protocols

Trading Partners who conduct business with Medicare are subject to CMS security policies.

CMS' information security policy strictly prohibits the sharing or loaning of Medicare assigned IDs and passwords. Users should take appropriate measures to prevent unauthorized disclosure or modification of assigned IDs and passwords. Violation of this policy will result in revocation of all methods of system access, including but not limited to EDI front-end access or EDC RACF user access. NGS is responsible for notifying all affected providers as well as reporting the system revocation to CMS. See the Appendix A CMSR High Impact Level Data document (**SA-9**) located on the CMS website at <https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS1248023.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending>

Upon registering with NGS for EDI or DDE services, NGS will provide a submitter or User ID and a default password. The default password will expire upon initial use to allow the user to define a unique password. See Section 2.2 for EDI registration procedures.

NGS has specific requirements for establishing passwords for both file transfer submitter IDs and RACF User IDs for access to the DDE application. These requirements are as follows:

- A.** The password length must be eight (8) characters.
- B.** Contain a combination of alpha and numeric characters.
- C.** Passwords must have at least one (1) of these special characters -- @, # or \$ --
- D.** Passwords must include at least one (1) uppercase and one (1) lowercase letter (case sensitive).
- E.** May not contain a four letter or greater 'dictionary' word, i.e., any word four letters or greater that can be found in a dictionary.
- F.** A minimum of four characters must be changed in each password reset.
- G.** May not be changed more than once in any 24 hour rolling period.
- H.** You should choose passwords that are easy for you to remember but hard for others to guess. One of the easiest ways to choose a password is to use the first letters of a phrase you can easily remember. For example, "I like to go to the dollar theater" could translate to "IL2GTT\$T." Other examples of acceptable passwords include SPR1NG\$4 and C@nad@01.
- I.** You should never write down your passwords or share them with anyone.
- J.** DDE RACF user IDs are revoked after three (3) consecutive unsuccessful password attempts.
- K.** Use of previous 12 passwords is prohibited. Reset passwords cannot be the same as any of the previous 12 passwords.
- L.** EDI Submitter ID passwords will expire after 60 days.
- M.** EDI Submitter IDs will suspend after 30 days of inactivity.
- N.** Inactive DDE RACF user IDs will auto revoke after 30 days. After 90 days of inactivity the DDE RACF user ID will be permanently deleted.
- O.** The DDE RACF passwords can only be reset one time a day. End-users must wait a minimum of one (1) day before they can change their own password again.
- P.** DDE RACF passwords expire after 30 days. Users are required to enter a new valid password upon receiving this prompt from the system.

V. Contact information

5.1 EDI Customer Service

- **EDI Help Desk:**
 - **J6:** 877-273-4334
 - **JK:** 888-379-9132
- **EDI Help Desk hours:** 7:00 a.m.-4:00 p.m. CT / 8:00 a.m.-5:00 p.m. ET
- Inquiries can be sent using the EDI Help Desk Email Inquiry Form found at <https://www.NGSMedicare.com>, select **Contact Us**, follow the link to the **EDI Help Desk Information**.

5.2 EDI Technical Assistance

- **EDI Help Desk:**
 - **J6:** 877-273-4334
 - **JK:** 888-379-9132
- **EDI Help Desk hours:** 7:00 a.m.-4:00 p.m. CT / 8:00 a.m.-5:00 p.m. ET
- Inquiries can be sent using the EDI Help Desk Email Inquiry Form found at <https://www.NGSMedicare.com>, select **Contact Us**, follow the link to the **EDI Help Desk Information**.

5.3 Provider Services

For questions on claims in the claim s systems or questions on remittance payments, contact the Provider Customer Care or the IVR number.

- **JK:**
 - **IVR:** 877-567-7205
 - **Toll-Free Number:** 888-855-4356
 - **TTY:** 866-786-7155
- **J6:**
 - **Illinois, Wisconsin, and Federally Qualified Health Centers:** **IVR:** 877-567-7206
 - **Toll-Free Number:** 877-702-990
 - **TTY:** 888-897-7523

Hours Available:

Monday – Friday, 7:00 a.m.-4:00 p.m. CT / 8:00 a.m.-5:00 p.m. ET

Thursdays closed for training: 1:00-3:00 p.m. CT / 2:00-4:00 p.m. ET

5.4 Applicable Websites/Email

Refer to Sections 1.4 and 1.5 for applicable websites and Section 5 for email contact.

VI. Control Segments / Envelopes

Reference	Name	Codes	Notes/Comments
ISA	Interchange Control Header		
ISA01	Authorization Information Qualifier	00	Medicare expects the value to be "00". ISA02 shall contain 10 blank spaces.
ISA02	Authorization Information	00	Medicare expects the value to be "00". ISA02 shall contain 10 blank spaces.
ISA03	Security Information Qualifier	00	Medicare expects the value to be "00" and ISA04 shall contain 2 blank spaces.
ISA04	Security Information		Medicare does not use Security Information; will ignore content sent in.
ISA05	Interchange ID Qualifier	28 27 ZZ	ISA05 = 28 or ZZ for 837I ISA05 = 27 or ZZ for 837P ISA05 = ZZ for 276
ISA06	Interchange Sender ID		NGS assigned Submitter ID. This is also required in the GS02 and 1000A.NM109 for 837
ISA07	Interchange ID Qualifier	28 27 ZZ	ISA07 = 28 or ZZ for 837I ISA07 = 27 or ZZ for 837P ISA07 = ZZ for 276
ISA08	Interchange Receiver ID		Institutional: California (HHH) 06014 Connecticut 13101 Illinois 06101 Maine 14011 Massachusetts 14211 Minnesota 06201 New Hampshire 14013 New York 13201 Rhode Island 14411 Vermont 14013 Wisconsin (incl. FQHC and HHH) 06001 HHH: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont only 14011 Professional: Connecticut 13102 Illinois 06102 Maine 14112 Massachusetts 14212 Minnesota 06202 New Hampshire 14312 New York (Upstate) 13282 New York (Downstate) 13202 New York (Queens) 13292 Rhode Island 14412 Vermont 14512 Wisconsin 06302 These Receiver IDs are also required in the GS03 and in Loop 1000A.NM109 for 837

Reference	Name	Codes	Notes/Comments
ISA11	Repetition Separator		Must Be Present
ISA14	Acknowledgment Requested	1	Medicare requires submitter to send code value 1 - Interchange Acknowledgment Requested (TA1). Medicare will only return a TA1 segment when there is an error in the ISA/IEA Interchange Envelope.
GS02	Application Sender Code		Include submitter number assigned by NGS.
GS03	Application Receiver's Code		Receiver ID assigned by NGS. Institutional: California (HHH) 06014 Connecticut 13101 Illinois 06101 Maine 14011 Massachusetts 14211 Minnesota 06201 New Hampshire 14013 New York 13201 Rhode Island 14411 Vermont 14013 Wisconsin (incl. FQHC and HHH) 06001 HHH: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont only 14011 Professional: Connecticut 13102 Illinois 06102 Maine 14112 Massachusetts 14212 Minnesota 06202 New Hampshire 14312 New York (Upstate) 13282 New York (Downstate) 13202 New York (Queens) 13292 Rhode Island 14412 Vermont 14512 Wisconsin 06302
GS08	Version Identifier Code	837I 005010X22 3A1 Errata 005010X22 3A2 837P 005010X22 2 Errata 005010X22 2A1 276 005010X21 2 No Errata Version Change	Errata Version when applicable. GS08 must also match the ST03

Reference	Name	Codes	Notes/Comments
NM109 837 - 1000A Loop 276 - 2100B Loop			Submitter ID. Must match the value submitted in ISA06 and GS02.
NM109 837 - 1000B Loop 276 - 2100A Loop			Receiver ID. Must match value submitted in ISA08 and GS03.

Interchange Control (ISA/IEA), Function Group (GS/GE), and Transaction (ST/SE) envelopes must be used as described in the national implementation guides. Medicare's expectations for inbound ISAs and a description of data on outbound ISAs are detailed in this chapter. Specific guidelines and instructions for GS and GE segments are contained in each Transaction Information Companion Guide.

Note: Medicare only accepts functional groups based upon one TR3 Implementation Guide per Interchange Envelope (ISA/IEA). If transactions based upon more than one TR3 Implementation Guide are being submitted, each must be contained within its own Interchange.

For Medicare FFS-specific guidance refer to the appropriate Medicare FFS transaction specific edit documents found at <https://www.cms.gov/Medicare/Billing/>.

6.1 ISA-IEA

Delimiters – Inbound Transactions

As detailed in the HIPAA-adopted implementation guides, delimiters are determined by the characters sent in specified, set positions of the ISA header. For transmissions to Medicare (inbound transmissions), these characters are determined by the submitter and can be any characters which are not contained within any data elements within the ISA/IEA Interchange Envelope.

Delimiters – Outbound Transactions

Medicare recommends the use of the following delimiters in all outbound transactions; trading partners/submitters should contact their local A/B MAC or CEDI, HHH-A for any deviations. Note that these characters will not be used in data elements within an ISA/IEA Interchange Envelope.

Delimiter	Character Used	Dec Value	Hex Value
Data Element Separator	>	62	3E
Repetition Separator	^	94	5E
Component Element Separator	+	43	2B
Segment Terminator	~	126	7E

Inbound Data Element Detail and Explanation

All data elements within the interchange envelop (ISA/IEA) must follow X12 syntax rules as defined within the adopted implementation guide.

6.2 GS-GE

Functional group (GS-GE) codes are transaction specific. Therefore, information concerning the GS/GE Functional Group Envelope can be found in the transaction specific appendices of this Companion Guide.

GS03 - Application Receiver's ID - NGS will reject an interchange (transmission) that is submitted with an invalid value in GS03 (Application Receivers Code) based on the intermediary definition.

GS06 - Group Control Number - Must be a unique (not previously submitted) and incremented number for each transaction submitted and must match the number in the GE02 segment

6.3 ST-SE

Medicare has no requirements outside the HIPAA-adopted transaction implementation guides.

NGS will only accept claim s for one line of business per transaction. Claims submitted for multiple lines of business within one ST-SE (Transaction Set) will cause the transaction to be rejected.

ST02 - Transaction Control Set - NGS will reject an interchange (transmission) that is not submitted with unique values in the ST02 (Transaction Set Control Number) elements.

VII. Acknowledgements and Reports

7.1 ASC X12 Acknowledgments

Medicare has adopted two new acknowledgement transactions, the 999 Implementation Acknowledgment for Health Care Insurance and the 277 Claims Acknowledgment or 277CA. These two acknowledgments will replace proprietary reports previously provided by NGS.

Medicare FFS has adopted a process to only reject claim submissions that are out of compliance with the ASC X12 version 5010 standard; the appropriate response for such errors will be returned on a 999 Implementation Acknowledgment transaction. Batch submissions with errors will **not** be rejected in totality, unless warranted, but will selectively reject the claims submitted in error within it. Thus, Medicare FFS will reject claim submissions and return a 999 Implementation Acknowledgment for reporting batch errors and 277CA for reporting claim errors.

7.2 Report Inventory

Transaction Acknowledgement (TRN) Report

The TRN is a text report file indicating initial validation of the inbound claims file, including whether or not a claims file was identified as being an ANSI file.

- The naming form is trn.(input filename).txt.##### where - ##### is a sequence number generated by EDI Systems
 - For example: **trn.TRANS.837.041313.txt.52731**
- For TRNs generated in response to transactions sent via the sFTP and the Internet Gateway with spaces in the file name “ABC 123 DEF”, the naming convention, will replace spaces with underscores and is as follows: TRN.ABC 123 DEF.##### (##### = 5-digit sequence number)
 - For example: **TRN.ABC_123_DEF.12345**
- The TRN will contain the Time Stamp, File Name, Trading Partner ID, and Original File size of the received claim file.
- The TRN will identify Internet Gateway transmission errors related to both the submission of the X.509 digital certificate data or file transfer activities.
- The file naming convention for the TRN generated for 276 files submitted **via the Internet Gateway** is as follows: “**TRN.COREBATCH.[payloadid].%s**” where [payloadid] is the payload ID from the originally submitted file and %s is the EDI assigned sequence number
- **Note:** The TRN reports generated for 276 files submitted via the Internet Gateway can only be accessed via the sFTP Gateway.

Transaction Acknowledgement (TA1)

- The TA1 segment indicates whether there are problems encountered with the X12 interchange control structure.
- The TA1 will not be returned if the originally submitted data was not recognized as an X12 formatted file.

- For TA1s generated in response to transactions sent via the sFTP and the Internet Gateway, the file naming convention is as follows: TA1.File Name.#### (4 digit sequence number)
 - For example:TA1.FileName.1234
- For TA1's generated in response to transactions sent via the sFTP and the Internet Gateway with spaces in the file name "ABC 123 DEF", the naming convention, will replace spaces with underscores and is as follows: TRN.ABC 123 DEF.#### (#### = 4-digit sequence number)
 - For example: **TA1.ABC_123_DEF.1234**
- The TA1 will return standard ANSI X12 reasons for the rejection of a submitted file based on control structures
- The TA1 will use the delimiters from the submitted file as the delimiters in the TA1.
 - For example, using > as the Component Element Separator in the inbound claims file will cause the TA1 to return the > as the Component Element Separator

Implementation Acknowledgement for Health Care Insurance (999)

- The 999 is an ANSI file indicating results of data integrity analysis of the claims file
- The naming form at is 999.(input file name).txt_000001.##### where ##### is the sequence number.
 - For example: **999.T RANS.837.041313.txt_000001.52745**
- The file naming convention for the 999 generated for a 276 file submitted via the **Internet Gateway** is as follows: "**999.COREBATCH.[payloadid].%s**" where the payload ID is the payload ID from the envelope of the 276 file submission.
- The 999 will return standard delimiters regardless of those used in the claims file
- If the 999 is rejected at the Functional Group Response Trailer (AK9), the 999 will instead return the delimiters used in the original submitted file.
- The 999 will be "wrapped," with all segments on one long line of data

Claims Acknowledgement (277CA)

- The 277CA is an ANSI X12 transaction indicating results of Medicare front end editing of the claims file
- The naming format is **277CA_X12.20170317 (date in CCYYMMDD) 004413 (time in HHMMSS).####**; where ##### is the sequence number.
- The 277CA will return standard delimiters regardless of those used in the claims file
- The 277CA will be "wrapped," with all segments on one long line of data

VIII. Additional Trading Partner Information

While NGS EDI Gateway is available 24/7, NGS schedules regular maintenance for Sundays. Access to the EDI Gateway may be interrupted while maintenance is performed.

8.1 Implementation Checklist

- Network Service Vendor Connectivity established for sFTP Gateway
- Practice Management Software supports current HIPAA versions of transaction sets.
- Practice Management Software supports translation of Acknowledgement Transactions
- EDI Enrollment and Registration Forms on file with NGS
- Submitter ID established or Provider Authorization Form submitted for third-party submitter

Accessing the Internet Gateway for 276/277 Claims Status/Response and 835 ERA Transactions:

- Obtain X.509 Digital Certificate if accessing the NGS Internet Gateway
- Submit X.509 Digital Certificate file to NGS sFTP Gateway
- Ensure software to support HTTP:MIME or SOAP/WSDL Protocol
- Appropriate URLs for Protocol

8.2 Transmission Examples: Control Segment Examples

5010 837 Professional

```
ISA*00*  *00* *ZZ*SENDERID  *27*13282 *100706*1100**^*00501*068490001*1*P*>~
GS*HC*SENDERID*13282*20100706*1100*4001*X*005010X222A1~
ST*837*000000001*005010X222A1~

SE*45*000000001~
GE*1*4001~
IEA*1*068490001~
```

5010 837 Institutional

```
ISA*00*  *00* *ZZ*SENDERID  *28*13101 *091222*1001**^*00501*355601000*1*T*>~
GS*HC*SENDERID*13101*20091222*1001*178001*X*005010X223A2~
ST*837*000000001*005010X223A2~

SE*31*000000001~
GE*1*178001~
IEA*1*355601000~
```

5010 276 Claim Status Request Professional

```
ISA*00*  *00* *ZZ*SENDERID  *27*13282 *100915*1828**^*00501*182827994*1*P*~:~
GS*HR*SENDERID*13282*20090915*1828*1*X*005010X212~
ST*276*6A92000Ax*005010X212~

SE*15*6A92000Ax~
GE*1*1~
IEA*1*182827994~
```

5010 276 Claim Status Request Institutional

ISA*00* *00* *ZZ*SENDERID *28*13101 *100915*1828*^*00501*182827994*1*P*:~
 GS*HR*SENDERID*13101*20090915*1828*1*X*005010X212~
 ST*276*6A92000Ax*005010X212~
 SE*15*6A92000Ax~
 GE*1*1~
 IEA*1*182827994~

5010 277 Claim Status Response - Professional

ISA*00* *00* *ZZ*13202 *29*13202 *100720*2135*^*00501*000000001*0*T*:~
 GS*HN*13202*SENDERID*20100720*21351929*32*X*005010X212~
 SE*18*000000001~
 GE*1*32~
 IEA*2*000000001~

5010 277 Claim Status Response - Institutional

ISA*00* *00* *ZZ*13101 *29*13101 *100720*2135*^*00501*000000001*0*T*:~
 GS*HN*13101*SENDERID*20100720*21351929*32*X*005010X212~
 SE*18*000000001~
 GE*1*32~
 IEA*2*000000001~

5010 835 Remittance – Professional

ISA*00* *00* *ZZ*13282 *29*SENDERID *101207*2115*^*00501*000000001*0*T*:~
 GS*HP*13282*SENDERID*20101207*21150222*1*X*005010X221A1~
 SE*909*0001~
 GE*1*1~
 IEA*1*000000001~

5010 835 Remittance – Institutional

ISA*00* *00* *ZZ*13101 *29*SENDERID *101207*2115*^*00501*000000001*0*T*:~
 GS*HP*13101*SENDERID*20101207*21150222*1*X*005010X221A1~
 SE*909*0001~
 GE*1*1~
 IEA*1*000000001

8.3 Trading Partner Agreement

EDI Trading Partner Agreements 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. Medicare FFS requires all Trading Partners to sign a Trading Partner Agreement with NGS. This agreement can be found at <https://www.NGSMedicare.com>.

Additionally, NGS requires the following:

- Submission of an EDI Registration Form when contracting with a third party (clearinghouse, billing service) to perform EDI transactions on behalf of a provider.

- NGS also requires obtaining connectivity to the NGS EDI Gateway through one of the NGS approved NSVs. A list of the NSVs can be found at <https://www.NGSMedicare.com>, select **the Claims & Appeals tab, > EDI Enrollment, > Network Service Vendors**

8.4 Frequently Asked Questions

FAQs can be accessed at

<https://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/index.html?redirect=/ElectronicBillingEDITrans> and on the NGS website at <https://www.NGSMedicare.com> select **the Claims & Appeals tab, any link**, then the **FAQs** are published at the bottom of each content section.

8.5 Other Resources

Refer to Sections 1.4, 1.5 and Section 10 for resources.

IX. Trading Partner Information Change Summary

Version	Date	Section(s) changed	Change Summary
1.0	November 5, 2010	All	Initial Draft
2.0	January 3, 2011	All	1st Publication Version
3.0	February 15, 2011	All	JK MAC Part A Specifications (CR7251)
3.0	April 2011	Section 7	Remove Loop/Segment Information
4.0	April 2017	All	Modifications for implementation of Internet Gateway
5.0	August 2017	All	Added TRN and TA1 file name convention changes, updated hyperlinks throughout document
6.0	July 2018	4.2	Changed Certificate Authority from Symantec to DigiCert

X. Appendices

- A** 837 Institutional Claim Transaction Specific Information
www.cms.gov/ElectronicBillingEDITrans/Downloads/5010A2837ACG.pdf
- B** 837 Professional Claim Transaction Specific Information
www.cms.gov/ElectronicBillingEDITrans/Downloads/5010A1837BCG.pdf
- C** 276/277 Claim Status Inquiry and Response Transaction Specific Information
www.cms.gov/ElectronicBillingEDITrans/Downloads/5010276277CG.pdf
- D** 835 Remittance Advice Transaction Specific Information
www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/Downloads/EDI-5010A1835CG.pdf