



MEDICARE
Electronic Data Interchange

**GENERAL COMPLETION INSTRUCTIONS FOR
NETWORK SERVICE AGREEMENT (NSA)**

ALL third party agents such as billing services, clearinghouses and Network Service Vendors (NSV) who represent Medicare providers that send and receive Medicare electronic transactions, **MUST** sign the Network Service Agreement.

Signature: THIS SECTION MUST BE COMPLETED. IF ALL OF THE INFORMATION IS NOT COMPLETE, YOUR EDI APPLICATIONS WILL BE RETURNED FOR ADDITIONAL INFORMATION.

Sole Proprietor or Company Name: Please provide the name of the billing service, clearinghouse or NSV.

Address: Please provide the address of the billing service, clearinghouse or NSV.

City, State, Zip: Please provide the city, state and zip code of the billing service, clearinghouse or NSV.

Telephone/Email: Please provide the telephone number and email address of who signed the NSA should additional contact be needed by Medicare EDI.

Signed By: Please have the billing service, clearinghouse or NSV sign the Network Service Agreement (NSA).

Printed Name: Please print the name of the individual who signed the NSA.

Title and Date: Please print the title of the individual who signed the NSA and the date.

Sender/Submitter (if applicable): Please provide the sender/submitter number of the billing service, clearinghouse or NSV. If you are applying for a new sender/submitter number, please leave blank.

Once the form has been completed, please submit the form to Medicare EDI. The form may be faxed to 904-361-0470 or mailed to Medicare EDI, 532 Riverside Avenue, Jacksonville, FL 32202.



MEDICARE
Electronic Data Interchange

Network Service Agreement

Third party agents that represent providers, including Network Service Vendors (NSV), certain value-added networks, clearinghouses, and billing agents that will send and receive Medicare electronic transactions, must sign an agreement that includes the following:

The third party provider agent agrees that:

1. All beneficiary-specific information is confidential and subject to the provisions of the Privacy Act of 1974, which required Federal information system to establish appropriate safeguards to ensure the security and confidentiality of individually identifiable records. This includes eligibility information, claims, remittance advice, online claims correction, and any other transactions where any individually identifiable information applicable to a Medicare beneficiary is processed or submitted electronically.
2. It has no ownership rights and is not a user of the data, but merely a means of transmitting data between users that have a need for the data and are already identified as legitimate users under a "routine use" of the system; that is, disclosure for purposes that are compatible with the purpose for which Medicare collects the information;
3. The beneficiary eligibility data submitted to them by the FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI are owned by Medicare.
4. It will not disclose any information concerning a Medicare beneficiary to any person or organization other than a.) an authorized Medicare provider making an inquiry concerning a Medicare beneficiary who is the provider's patient, b.) CMS or c.) FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI.
5. It will promptly notify the FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI of any unauthorized disclosure of information about a Medicare beneficiary and will cooperate to prevent further unauthorized disclosure;
6. The data will not be stored for any duration longer than that required to assure that they have reached their destination, and no more than 30 days for any purpose;
7. It has identified to the FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI in writing of any instances where it would need to view Medicare data in order to perform its intended tasks under the agreement. It will not view the data unless it is absolutely necessary to perform its intended tasks.
8. It will not prepare any reports, summary or otherwise, based on any individual aspect of the data content. For example, data cannot be viewed or manipulated by connectivity vendors to create reports for providers, that function is reserved for a provider's clearinghouse or billing service. Reports may be written, however, on data externals or summaries such as the number of records transmitted to a given receiver on a given date.
9. It will guarantee that an authorized user may be deleted within 24 hours in the event that person leaves their employment, no longer has a need to access this information, or there is a possible security breach.
10. No incoming or outgoing electronic data interchange (EDI) will be conducted unless authorization for access is in writing, signed the provider, submitted to the provider's FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI, and each provider has a valid EDI Enrollment form on file with that CMS contractor.

11. It has safeguards in place to assure each eligibility response is sent only to the provider that initiated the inquiry;
12. It has safeguards in place to assure that all other outbound transactions such as the TA1 interchange acknowledgment, 999-E accepted functional groups/transaction sets with errors, 999-R rejected functional groups/transaction sets, 999-A clean functional acknowledgments 277CA claims acknowledgment, ANSI 835 electronic remittance advice, and the ANSI 277 claim status inquiry response received from the FI, Carrier, RHHI, A/B MAC or CEDI are sent only to the appropriate authorized entity.
13. It will furnish, upon request, documentation that assures the above privacy and security concerns are being met;
14. It will adhere to the regulations on security and privacy standards for health information under the Health Insurance Portability and Accountability Act of 1996; *and extended to all business associates of a covered entity per ARRA.*
15. It will require its subcontractors, agents, and business associates to comply with all applicable current requirements of this agreement as well as any future requirements or changes to this agreement; and
16. It will comply with CMS Internet policy. (CMS does not permit the transmission of protected health data between providers and other parties who are not Medicare contractors over the Internet unless it is authenticated and encrypted. The CMS policy requires written notification of intent from organizations anticipating use of the Internet. The CMS reserves the right to require the submission of documentation to demonstrate compliance with requirements or to conduct on-site audits to ascertain compliance).

NOTE: Federal law shall govern both the interpretation of this document and the appropriate jurisdiction and venue for appealing any final decision made by CMS under this document. This document shall become effective when signed by the third part agent. The responsibilities and obligations contained in this document will remain in effect as long as electronic data interchange is being conducted with an FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI. Either party may terminate this arrangement by giving the other party thirty-days (30) notice of its intent to terminate.

SIGNATURE: (all fields required)

I certify that I have been appointed an authorized individual to whom the provider has granted the legal authority to enroll it in the Medicare Program, to make changes and/or updates to the provider's status in the Medicare Program (e.g., new practice locations, change of address, etc.) and to commit the provider to abide by the laws, regulations and the program instructions of Medicare. I authorize the above listed entities to communicate electronically with (MAC name) on my behalf.

Sole Proprietor
or Company
Name

Address

City, State, Zip

Telephone/Email

Signed By

Printed Name

Title

Date

Sender/Submitter
(If applicable)

FI, Carrier, RHHI, A/B MAC, DME MAC or CEDI to whom this is being submitted:

Mailing Address:

Medicare EDI
PO Box 44071 – 3C
Jacksonville, FL 32231-4071

Phone and Fax Numbers:

Phone: 1-888-670-0940, option 4
Fax: 904-361-0470

Physical Address:

Medicare EDI
532 Riverside Ave. 3C
Jacksonville, FL 32202-4918