

# Network Service Vendor (NSV) Agreement

## 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 requires Federal information systems 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 transaction 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;
2. The beneficiary data submitted to them by the A/B MAC, DME MAC or CEDI are owned by Medicare;
3. 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) CMS' A/B MAC, DME MAC or CEDI;
4. It will promptly notify the 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;
5. 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;
6. It has identified to the 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;
7. 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;
8. 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;
9. No incoming or outgoing electronic data interchange (EDI) will be conducted unless authorization for access is in writing, signed by the provider, submitted to the provider's A/B MAC, DME MAC or CEDI and each provider has a valid EDI enrollment form on file with that CMS contractor;
10. It has safeguards in place to assure each eligibility response is sent only to the provider that initiated the inquiry;
11. It has safeguards in place to assure that all other outbound transactions such as the TA1 interchange acknowledgment, ASC X12 999-E implementation acknowledgment accepted functional groups/transaction sets with errors, ASC X12 999-R implementation acknowledgment rejected functional groups/transaction sets, ASC X12 999-A implementation acknowledgment clean functional acknowledgments, ASC X12 277CA claim acknowledgment, ASC X12 835 electronic remittance advice, and the ASC X12 277 claim status request response received from the A/B MAC or CEDI are sent only to the appropriate authorized entity;

implementation acknowledgment clean functional acknowledgments, ASC X12 277CA claim acknowledgment, ASC X12 835 electronic remittance advice, and the ASC X12 277 claim status request response received from the A/B MAC or CEDI are sent only to the appropriate authorized entity;

12. It will furnish, upon request, documentation that assures the above privacy and security concerns are being met;

13. It will adhere to the regulations on security and privacy standards for health information under HIPAA, and extended to all business associates of a covered entity per ARRA (see section 20 above for a review of these legislative references);

14. 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

15. 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 party agent. The responsibilities and obligations contained in this document will remain in effect as long as electronic data interchange is being conducted with an A/B MAC, DME MAC or CEDI. Either party may terminate this arrangement by giving the other party thirty (30) days notice of its intent to terminate.

**SIGNATURE:** The signatory hereto represents and warrants that he/she is duly authorized to sign, execute, and deliver this Agreement on behalf of the party it represents for the Medicare Program 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 Code:

Signed By:

---

NSV Signature

Type Name:

Title:

Date:  Trading Partner ID (if known):

Carrier, DMERC, FI/other contractor if designated by CMS to whom this is being submitted (**to be completed by EDISS**):

Contractor Signature: \_\_\_\_\_

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