Medicare
Carriers Manual
Part 3 - Claims Process

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal 1749 **Date: APRIL 26, 2002**

CHANGE REQUEST 2057

HEADER SECTION NUMBERS	PAGES TO INSERT	PAGES TO DELETE
Table of Contents	3-1 - 3-1.1 (2 pp.)	3-1 - 3-1.1 (2 pp.)
3021.2 - 3021.4 (Cont.)	3-17 - 3-17.3 (4 pp.)	3-17 - 3-17.3 (4 pp.)
3021.6 - 3022	3-17.6 - 3.17.10 (5 pp.)	3-17.6 - 3-17.9 (4 pp.)

NEW/REVISED MATERIAL--*EFFECTIVE DATE: May 1, 2002*
IMPLEMENTATION DATE: July 1, 2002

This transmittal amends the Network Service Agreement to extend the Network Service Agreement requirements to agents and subcontractors of vendors, agents, subcontractors, and business associates who exchange electronic data interchange transactions with CMS or its Medicare Part B carriers.
It also instructs carriers on the policy for notification by providers of provider/vendor contract changes.
This transmittal also amends the instructions for security-related requirements to prohibit carriers from requiring that providers/vendors send unique USERIDs and Passwords with eligibility transactions.

Section 3021.3, Security-Related Requirements for Subcontractor Arrangements With Network Services.--Carriers may not require that providers/vendors submit unique USERIDs and passwords within eligibility inquiry transactions. Carriers are responsible for the privacy and security of eligibility data sent directly from providers, and must be able to associate all inquiries with providers. Eligibility verification vendors are responsible for the privacy and security of the providers that contract with them for eligibility information, and must be able to associate all inquiries with providers.

Section 3021.7, Advise Your Providers and Network Service Vendors.--Medicare Part B carriers must maintain current information on the status of provider/vendor contracts.

Section 3021.8, Network Service Agreement.--extend Network Service Agreement requirements to vendor subcontractors, agents, and business associates, and their subcontractors, agents, and business associates; and prohibit network service vendors, vendor subcontractors, agents, and business associates, and their subcontractors, agents, and business associates from requiring that providers or their representatives send unique USERIDs and passwords within eligibility transactions. The addenda require compliance by vendor subcontractors, agents, and business associates, and their subcontractors, agents, and business associates with all current Network Service Agreement requirements as well as any future requirements or changes to the Network Service Agreement.

Section 3021.9, Notification to Providers and Eligibility Verification Vendors.--Providers and eligibility verification vendors must be notified by May 1, 2002.

Disclaimer: The revision date and transmittal number only apply to the redlined material. All other material previously was published in the manual and only is being reprinted.

These instructions should be implemented within your current operating budget.

CHAPTER III
CLAIMS, FILING, JURISDICTION
AND DEVELOPMENT PROCEDURES

Section

Filing the Request for Payment

Electronic Data Interchange

CHAPTER III
CLAIMS, FILING, JURISDICTION AND DEVELOPMENT PROCEDURES

Section

Electronic Media Claims

3021. ELECTRONIC DATA INTERCHANGE SECURITY, PRIVACY, AUDIT AND LEGAL ISSUES

3021.1 Contractor Data Security and Confidentiality Requirements.--All Medicare beneficiary-specific information is confidential and subject to the requirements of §1106(a) of the Social Security Act (the Act) and implementing regulations at 42 CFR Part 401, Subpart B. Those regulations specify that, as a general rule, every proposed disclosure of Medicare information shall be subject to the Freedom of Information Act rules at 45 CFR Part 5. Also, all such information, to the extent that it is maintained in a "system of records," is protected under the provisions of the Privacy Act of 1974 (5 U.S.C. 552a) and implementing regulations at 45 CFR Part 5b. Such information is included in claims, remittance advice, eligibility information, online claims corrections, and any other transactions where medical information applicable to an individual is processed or transported. Such information may not be disclosed to anyone other than the provider, supplier, or beneficiary for whom the claim was filed. (See §3021.3 for implications on Network Services.) Ensure the security of all electronic data interchange (EDI) transactions and data. (See §§5135-5139.) Include the following security capabilities in your system:

- Make sure that all data are password protected and that passwords are modified at periodic but irregular intervals, when an individual having knowledge of the password changes positions, and when a security breach is suspected or identified;
- Provide mechanisms to detect unauthorized users and prohibit access to anyone who does not have an appropriate user ID and password;
- Maintain a record of operator-attempted system access violations;
- Maintain a multi-level system/user authorization to limit access to system functions, files, databases, tables, and parameters from external and internal sources;
- Maintain updates of user controlled files, databases, tables, parameters, and retain a history of update activity; and
- Protect data ownership and integrity from the detailed transaction level to the summary file level.

3021.2 EDI Audit Trails.--Maintain an automated transaction tracking and retrieval capability and retain an audit trail of on-line and batch transaction experience(s) affecting the complete processing of a claim from date of receipt to date of payment or denial and any subsequent adjustments.

You must be able to retrieve:

- The claim as received from the provider of health care services, physician, supplier, or billing service;
- The claim as paid to the provider of health care services, physician, or supplier;
- All adjustments made on the claim;
- The check or the electronic funds transfer (EFT) record sent to the provider of health care services, physician, or supplier; and
- The remittance advice as sent to the provider of health care services, physician, or supplier.

Maintain the ability to cross-refer all needed transactions to each claim being processed. The records may be kept on electronic, computer-output-microfilm, or optical disk media. Never ever allow anyone to overlay or erase a record. Each record must be kept intact. All records must be archived in accordance with the instructions in the MCM, Part 2, §5404.

It is important to have a well defined system for maintaining audit trail data so that you can demonstrate that data integrity is maintained at all times.

3021.3 Security-Related Requirements for Subcontractor Arrangements With Network Services.--A *network service* is any entity other than a billing service or clearinghouse engaged in EDI with a carrier or intermediary, on behalf of Medicare providers. Network services may not view privacy-protected Medicare data unless it is necessary to perform its intended tasks. For EDI, that would be any transaction in which either a beneficiary or a provider may be identified.

Some health care providers retain multiple billing services, vendors, and/or network services. Carriers may support multiple services if their system can protect Medicare data from unauthorized use. Each billing service, vendor, and network service may access only its own information. As an example, a provider has a network service for eligibility inquiry, a billing service for initial claims, and a vendor for denied claims. The provider reserves claim status and remittance advice for its internal staff. The billing service may access any claims it submitted on behalf of the provider, and it may perform all of the functions the provider may perform, if the provider so designates. The eligibility network service may send eligibility inquiries from the provider, and return responses, but it may not view the data, store it, or use it for any reports. The vendor for denied claims may have no access since they do not submit initial claims, and works directly with the provider for denied claim information. When supporting multiple billing services, vendors, and network services, carriers' systems must be capable of ascertaining that network services do not access, view, or use unauthorized Medicare information

Authorization for access to Medicare claims data must be in writing and signed by the provider. Each provider must sign a valid EDI enrollment form. A separate password is to be used for each provider's access.

A *vendor* provides hardware, software and/or ongoing support for total office automation or submission of EDI transactions directly to individual insurance companies. Vendors have no need to access Medicare data. Rather, they supply the provider the means for such access.

An *eligibility verification* vendor is to be treated as a network service;

A *clearinghouse* transfers or moves EDI transactions for a provider and translates the provider data into the format required by a health care trading partner, such as a payer. A clearinghouse accepts multiple types of claims and generally other EDI transactions and sends them to various payers, including Medicare. A clearinghouse also accepts EDI transactions from payers for routing to and/or reformatting for providers. Clearinghouses perform general and payer-specific edits on claims, and usually handle all of the transactions for a given provider. Clearinghouses frequently reformat data for various payers, and manage acknowledgements and remittance advice. Clearinghouses ordinarily submit initial claims, and may qualify as billing services.

A *value added network* (VAN) is a conduit to transfer or move EDI transactions for a provider. The owner of the VAN is not allowed to read the contents of files containing beneficiary- or provider- specific information. VAN owners are treated as network services.

A billing service offers claims billing services to providers. The billing service collects the providers' claim information and bills the appropriate insurance companies, including Medicare. It may provide claims billing services only, or provide full financial accounting and/or other services. Billing services may view beneficiary or provider data to perform their obligations to the provider, and if the provider designates them for that access. To qualify as a billing service, the entity must submit initial claims on the provider's behalf.

A *collection agency* is a service that bills after the original biller. Do not service collection agencies. Regardless of the title of an entity, authorization is determined according to the services performed by an entity rather than its title. A company that calls itself a VAN, but performs clearinghouse services, is treated as a clearinghouse for data access purposes. A company that calls itself a clearinghouse, but does not furnish translation or reformatting services, and merely transfers data as received between trading partners is treated as a VAN for data access purposes.

If the contractor enters into a written agreement for network services, then any such agreement must specify that:

- The data submitted to the network service by the contractor are owned by Medicare;
- The data are not stored for any duration longer than that required to assure that the data have reached the appropriate destination, and no more than 30 days for any purpose;
- The network service is not to view the data unless it is necessary to perform its intended tasks. In the event any data is viewed, perhaps for routing purposes, the network service is limited to viewing only those data needed for that purpose, and must strictly regulate access to that data;
- The network service is not to prepare any reports, summary or otherwise, based on any aspect of the data content. Reports may be written, however, on data externals such as the number of records transmitted to a given receiver on a given date;
- All services must guarantee that a user may be deleted within 24 hours. Other standards of performance, including, but not limited to, how quickly a user may be added to the network, must be specified in writing;
- Passwords are to be changed more frequently than required by the network service, and on a schedule that is difficult to predict;
- No incoming or outgoing EDI may be conducted unless there is a valid EDI enrollment form on file for the individual health care provider; and
- The lists of physicians, suppliers, and providers that have access are to be reviewed periodically to ensure that only authorized users have access.

3021.4 Electronic Data Interchange (EDI) Enrollment Form.--Arrangements for use of EDI with Medicare are specified in the CMS standard Electronic Data Interchange (EDI) Enrollment Form. This agreement must be executed by each provider of health care services, physician, or supplier that transfers data electronically with Medicare. Each EDI provider must sign the CMS standard EDI Enrollment Form and submit it to you before you accept the first electronic transaction for that provider. You must verify the existence of a valid EDI Enrollment form at the front end, prior to acceptance of an electronic bill or any other EDI transaction from a provider. This applies whether the provider submits transactions directly, or through a clearinghouse or other entity which has been issued an EDI submitter number. Notify third party agents that they are prohibited from submitting EDI transactions for customers/providers who have not yet filed a valid EDI Enrollment Form with you.

An organization comprised of multiple components that have been assigned Medicare provider numbers may elect to execute a single EDI Enrollment Form on behalf of the organizational components to which such numbers have been assigned. The organization as a whole is to be held responsible for the performance of its components.

The actual EDI Enrollment Form to be signed is as follows:

ELECTRONIC DATA INTERCHANGE (EDI) ENROLLMENT FORM

The provider agrees to the following provisions for submitting Medicare claims electronically to CMS or to CMS's contractors.

A. **The Provider Agrees**:

1. That it will be responsible for all Medicare claims submitted to CMS by itself, its employees, or its agents.

2. That it will not disclose any information concerning a Medicare beneficiary to any other person or organization, except CMS and/or its contractors, without the express written permission of the Medicare beneficiary or his/her parent or legal guardian, or where required for the care and treatment of a beneficiary who is unable to provide written consent, or to bill insurance primary or supplementary to Medicare, or as required by State or Federal law.

3. That it will submit claims only on behalf of those Medicare beneficiaries who have given their written authorization to do so, and to certify that required beneficiary signatures, or legally authorized signatures on behalf of beneficiaries, are on file.

4. That it will ensure that every electronic entry can be readily associated and identified with an original source document. Each source document must reflect the following information:

- Beneficiary's name,
- Beneficiary's health insurance claim number,
- Date(s) of service,
- Diagnosis/nature of illness, and
- Procedure/service performed.

5. That the Secretary of Health and Human Services or his/her designee and/or the contractor has the right to audit and confirm information submitted by the provider and shall have access to all original source documents and medical records related to the provider's submissions, including the beneficiary's authorization and signature. All incorrect payments that are discovered as a result of such an audit shall be adjusted according to the applicable provisions of the Social Security Act, Federal regulations, and CMS guidelines.

6. That it will ensure that all claims for Medicare primary payment have been developed for other insurance involvement and that Medicare is the primary payer.

7. That it will submit claims that are accurate, complete, and truthful.

3021.5 Information Regarding the Release of Medicare Eligibility Data.—The CMS is required by law to protect all Medicare beneficiary-specific information from unauthorized use or disclosure. Disclosure of Medicare beneficiary eligibility data is restricted under the provisions of the Privacy Act of 1974. The CMS's instructions allow release of eligibility data to providers or their authorized billing agents for the purpose of preparing an accurate claim. Such information may not be disclosed to anyone other than the provider, supplier, or beneficiary for whom the claim was filed. In order to strengthen the security of this data and to protect the privacy of our Medicare beneficiaries, we have added some additional safeguards to the existing guidelines.

We are limiting the way eligibility data is being accessed by network service vendors. For information regarding network service vendors, review §3021.3. You must give access to any network service vendor that requests access to eligibility data on behalf of providers as long as they adhere to the following rules:

- Each network service vendor must sign the new Network Service Agreement below;
- Each provider must be an electronic biller and must sign a valid Electronic Data Interchange (EDI) Enrollment Form;
- The provider must explain the type of service furnished by its network service vendor in a signed statement authorizing the vendor's access to eligibility data; and
- The network service vendor must be able to associate each inquiry with the provider making the inquiry. That is, for each inquiry made by a provider through a network service vendor, that vendor must be able to identify the correct provider making the request for each beneficiary's information.

3021.6 New Policy on Releasing Eligibility Data.--Beginning July 1, you must make the following changes. All work must be completed by January 31, 2001.

A. All providers and network service vendors must negotiate with a carrier for access to eligibility data. All contracts or business arrangement to access Medicare information made by providers and vendors with data centers must be terminated and renegotiated with the carrier.

B. All providers and network service vendors who are directly connected to data centers for eligibility access must be disconnected and rerouted through the carrier's front end software (which in some cases is operated at a data center location).

C. If you have made special arrangements for network service vendors to enhance their services such as installing their own special software, creating special code, or modifying CWF eligibility data, etc., then all existing special arrangements or codes must be discontinued. You must migrate all vendors and providers to the regular non-customized online process. You must not make any more special arrangements for providers or network service vendors.

D. You will discontinue allowing vendors and providers to go to one carrier to access all eligibility information. Vendors and providers may receive access to eligibility data only from the carrier to which the provider is assigned.

E. When an inquiry enters into your system, you must be able to ensure that:

- An EDI agreement has been signed by the provider;
- A network service agreement has been signed by the vendor; and
- Each inquiry can be identified by provider.

F. The eligibility data that providers receive from carriers must be either the CMS standard Part B flat file or the ANSI ASC X12 270/271 transaction sets. No other data, e.g., local history, Part A CWF eligibility data, etc, shall be substituted for eligibility information. You must terminate any eligibility data that is not either the standard Part B flat file or the ANSI ASC X12 270/271.

G. Providers may use eligibility data only for the approved use of preparing accurate claims. Access to eligibility data must be limited to individuals who support this function.

3021.7 Advise Your Providers and Network Service Vendors.—Carriers must maintain current eligibility access information. Providers must provide carriers written notice of any changes to their vendor contracts within 30 days of the effective date for the changes. Contractual changes include, but are not limited to:

- Change in vendors;
- Vendor ceases operations;
- Vendor is purchased by, or merged/aligned with another vendor or organization;
- Change in services provided by a vendor; and
- Discontinued use of vendor services by a provider.

When a new provider/vendor contract is initiated, or an existing contract changes for any of the above reasons, or another reason, written notification must be submitted to the appropriate contractors within 30 days of the effective date of the changes.

Notification includes vendor name and address identification and vendor tax identification number.

Notification may consist of the following:

- A new contract with termination notification for prior contract;
- Addenda to existing contracts; and
- Contract termination.

Carriers must contact all providers and network service vendors to advise them of these new procedures and their effective dates.

Carriers must remind providers that they must notify carriers when they change from one network service vendor to another, cease arrangements with a network service vendor, or leave the Medicare program. Adjustments must be made to the carriers' systems to reflect these changes.

3021.8 Network Service Agreement.--All current and new network service vendors must sign the following Network Service Agreement. No network service vendor will be able to continue to service providers for eligibility access if this agreement is not signed. Please add the following agreement to your existing contract.

All beneficiary-specific information is confidential and subject to administrative, technical, and physical 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 individually identifiable information applicable to a Medicare beneficiary is processed or submitted electronically.

Criminal penalties are up to $50,000 and 1 year in prison for obtaining or disclosing protected health information; up to $100,000 and up to 5 years in prison for obtaining protected health information under false pretenses; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

The word "it" when referring to a network service includes the employees of the service as well as the entities and individuals with whom the network service contracts.

The network service agrees that:

1. It has no ownership rights and is not a user of the data, but merely a conduit for transmission of 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. The CMS's Internet Policy prohibits the transmission of health care information between Medicare carriers/intermediaries and providers over the Internet. The CMS requires the use of private networks or dial-up connections between any provider/vendor and a Medicare contractor for the electronic transmission of all health care information.

2. The data submitted to the network service by the contractor 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 carriers or intermediaries.

4. It will promptly notify the contractor 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 contractor in writing 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. 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. Other standards of performance, including, but not limited to, how quickly a user may be added to the network, must be specified in writing.

9. No incoming or outgoing electronic data interchange (EDI) will be conducted unless authorization for access is in writing and signed by the provider, and each provider has a valid EDI enrollment form on file.

10. It has the ability to associate each inquiry with the provider making the inquiry, but may not require the provider to send unique USERIDs and passwords within the 270 eligibility inquiry transactions, once legitimate access is established.

11. It will furnish, upon request, documentation that assures the above privacy concerns are being met.

12. It understands the final regulation on Privacy and that the final regulation on Security Standards for health information under the Health Insurance Portability and Accountability Act of 1996 will be forthcoming. It will adhere to those regulations when they become effective.

13. It will require its subcontractors, agents, and business associates to:

- Comply with all applicable current requirements of the Network Service Agreement as well as any future requirements or changes to the Network Service Agreement.
- Require their subcontractors, agents, and business associates to comply with all applicable current requirements of the Network Service Agreement as well as any future requirements or changes to the Network Service Agreement.

14. The CMS does permit the transmission of protected health data between providers and other parties who are not Medicare contractors over the Internet if 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.

NOTICE:

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 network service. The responsibilities and obligations contained in this document will remain in effect as long as electronic data interchange is being conducted with CMS or the contractor. Either party may terminate this arrangement by giving the other party (30) days notice of its intent to terminate.

SIGNATURE:

I am authorized to sign this document on behalf of the indicated party and certify that I have read and agree to the forgoing provisions and acknowledge same by signing below.

Network Service Company Name

_____

Address

_____

City/State/Zip

_____

Signed By

_____

Title

_____

Date

_____

Contractor

_____

3021.9 Notification to Providers and Eligibility Verification Vendors—By May 1, 2002, carriers must notify eligibility verification vendors of these changes in a regularly scheduled provider bulletin or newsletter.

3022. MAINTAINING A DIRECTORY OF ELECTRONIC BILLING VENDORS

Publish and maintain a directory of your electronic billing vendors. Update the directory at least once annually and make it available to your providers (depending on their automation) either through your WEB page, electronic bulletin board, diskette, or hardcopy. Your provider bulletin can be used as hardcopy, when feasible. Use a disclaimer statement in the directory stating that the information is subject to change after the date of publication. Information should minimally include company name, phone number and mailing address. You may provide additional detail.

Conduct at least two meetings annually with all of your electronic billing vendors in order to brief them on planned Medicare eligibility, coverage, payment, and billing changes.