



MLN Matters®



Information for Medicare Fee-For-Service Health Care Professionals

Related Change Request (CR) #: N/A

MLN Matters Number: SE0461

Related CR Release Date: N/A

Inappropriate Access to or Use of Electronic Data Interchange (EDI) Transaction Data by Third Party Entities

Note: This article was updated on April 9, 2013, to reflect current Web addresses. All other information remains unchanged.

Provider Types Affected

All physicians, suppliers, and providers.

Provider Action Needed



STOP – Impact to You

Failure to abide by Medicare security requirements for EDI access could lead to suspension of EDI capabilities.



CAUTION – What You Need to Know

This article clarifies and reminds affected physicians, providers, and suppliers of existing Medicare requirements and prohibitions concerning use of EDI numbers and passwords.



GO – What You Need to Do

Be sure you and your third party partners are aware of and abide by these requirements to protect your EDI access and to maintain your ability to submit timely claims to Medicare.

Background

Medicare contractors (carriers and intermediaries) support electronic data interchange (EDI) to enable providers, either directly or through third party agents to:

- Verify patient eligibility to determine if a claim should be submitted to Medicare;
- Submit claims to Medicare electronically;
- Determine the status of a previously submitted claim; and

Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

- Post adjudication decisions and payments to patient accounts.

It is important to note that these functions are **the only functions** for which a provider or a third party entity is entitled to send EDI transactions directly to Medicare contractors (carriers, DMERCs, or fiscal intermediaries) or receive EDI transactions directly from Medicare contractors.

Third-party entities that request permission to access Medicare EDI records directly generally fall into one of the following categories:

1. A clearinghouse as defined by the Health Insurance Portability and Accountability Act (HIPAA) that transfers and may translate claim, eligibility, claim status, and/or payment and remittance advice data for EDI transactions being transmitted between providers and one or more Medicare contractors;
2. An agent a provider has hired to prepare claims and possibly other EDI transactions for submission to one or more Medicare contractors, and possible posting to patient records/provider accounts of eligibility, claim status, and adjudication/payment data issued by one or more Medicare contractors;
3. A clearinghouse as in #1 above that also performs agent services as in #2 above; and
4. A third party that does not perform clearinghouse or agent services as described in #1-3, but that may want direct access to outbound Medicare EDI transactions for alternate functions. Entities included in this category include collection agents in pursuit of delinquent beneficiary payments to providers and vendors that market payment data analysis services to providers that serve Medicare patients.

Third parties in categories 1, 2, and 3 perform functions that qualify them for direct access to Medicare contractor EDI systems. If a provider elects to use the services of a third party to perform permitted Medicare EDI functions, the provider must complete an EDI Agreement and furnish the Medicare contractor with a signed authorization specifying the EDI services each third party may perform on their behalf. The third party must comply with existing requirements to obtain their own EDI number and password from the Medicare contractor that services each provider being represented.

Medicare contractors can issue EDI numbers and passwords to category 1, 2, and 3 entities and permit them to submit and/or obtain EDI data directly to/from the Medicare contractor EDI systems. Third parties in category 4 do not perform functions that qualify them for direct access to Medicare systems, and may not be issued EDI numbers or passwords.

Medicare requires that providers and third party entities to which EDI numbers and passwords are issued protect the security of those numbers and passwords to prevent use by unauthorized individuals. Furthermore, providers and third party entities of any category are prohibited from accessing Medicare systems using an EDI number or password not directly issued to them by a Medicare contractor.

This instruction is being issued to clarify and remind affected parties of existing CMS requirements and prohibitions concerning access to and use of EDI numbers and passwords.

Issues

Although they may qualify for direct access to Medicare contractor EDI systems, the read, write and use rights vary for entities in categories 1, 2, and 3. Third parties in categories 2 or 3 are allowed to review data within transactions, whereas category 1 entities are limited to review of "electronic envelope" data that

Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

contains routing information for the transactions. Some category 1 entities may be confused regarding this limitation.

The Centers for Medicare & Medicaid Services (CMS) recently discovered that at least one third-party entity in category 4 has been using EDI numbers and passwords furnished them by providers to download electronic remittance advice (ERA) transactions for those providers. The data **was not being used** to post adjudication and payment data to patient accounts, but was being used solely for automated analysis to detect information such as payment patterns and to generate reports. The providers were using the paper remittance advice notices they received, and not the ERAs, to post their accounts. CMS has been advised that other companies may also be marketing similar services and may be using EDI numbers and passwords issued to providers to obtain outbound EDI transactions from Medicare contractor systems for use in ways other than intended by Medicare.

CMS Policy

The following manual instructions contain CMS requirements that apply to these issues:

- The Medicare Claims Processing Manual (Pub. 100-04, Chapter 24 (EDI Support Requirements) contains CMS requirements for EDI access. This can be accessed at <http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/clm104c24.pdf> on the CMS website.
- The Business Partners Systems Security Manual (BPSSM) (Appendix A, Section 2.9.10 of the Core Security Requirements (CSR)) contains further requirements applicable to use of passwords issued to permit system access. These can be found at http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/117_systems_security.pdf on the CMS website.
- These password requirements apply to entities to which Medicare contractors issue passwords, as well as to Medicare contractors themselves.
- The Medicare Claims Processing Manual (Pub. 100-04), Chapter 24 (EDI Support Requirements), Section 90 contains instructions concerning mandatory electronic submission of claims to Medicare as required by ASCA. This information is available at <http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/clm104c24.pdf> on the CMS website.
- The Medicare Claims Processing Manual (Pub.100-04), Chapter 1 (General Billing Requirements), Section 80 (Carrier and FI Claims Processing Timeliness) contains Medicare's payment floor requirements at <http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/clm104c01.pdf> on the CMS website.

In regard to access policies for entities in categories 1-4:

- Category 1 third parties that transfer EDI data to and/or from providers, but do not translate that data into or from a format that complies with the HIPAA requirements are **not permitted** to:
 - Open the electronic envelope of the transmitted data; or
 - Generate reports that include data from within those transmission envelopes.
- Category 2 and 3 agents **are permitted** to:

Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

- Open the electronic envelopes of the transmitted data; and
- Use the data for analysis and generation of reports for the providers they serve, in addition to use of that data to prepare beneficiary claims, determine claim status or Medicare eligibility, and/or to post adjudication and payment data to patient accounts.
- Category 4 third parties may use data prepared by Medicare, but the following requirements must be met as conditions for use:
 - The data must be forwarded to the entity by the provider;
 - A signed agreement must be in effect between the provider and the entity in which the provider authorizes the entity to use the data and specifying how the data may and may not be used;
 - The entity has furnished the provider with a signed confidentiality agreement that meets Medicare's and HIPAA's privacy and security requirements for protection of personally identifiable beneficiary health data;
 - The provider has notified the patients that their personally identifiable health data will be shared with the entity and how it will be used; and
 - The provider agrees not to furnish data to the entity for any patients who object.
- A category 4 entity:
 - May **not** be given an EDI number or password for direct access to Medicare data; and
 - Is never permitted to use a provider's EDI number or password for that or any other purpose.

As stated in the CSRs in BPSSM section 2.9.10, passwords (1) are "unique for specific individuals," (2) must be "controlled by the assigned user and [are] not subject to disclosure."

Contractor Actions if Improper Access is Identified

In the event a Medicare contractor becomes aware that improper access has been given, appropriate termination of EDI capabilities and notification must occur. For example:

- If an entity, previously issued an EDI number and password, falls under category 4, the Medicare contractor must immediately disable the EDI number and password of that entity, and then notify the entity and the provider why this has been done.
- If a third party entity is using a provider's EDI number and password to access Medicare systems, the Medicare contractor must immediately disable the EDI number and password, and then contact that provider by mail or phone to make them aware of Medicare's requirements and prohibitions.

During this contact, and while the EDI number and password are disabled, the Medicare contractor will remind the provider that:

- Loss of EDI privileges could result in termination of Medicare payment since the Administrative Simplification Compliance Act (ASCA) prohibits payment of claims submitted on paper that should have been submitted to Medicare electronically; and

Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

- In those cases when ASCA permits claims to be submitted on paper, payment is delayed as result of the lengthier payment floor that applies to paper claims.

Additional Information

Providers can review appropriate requirements by checking the Web sites mentioned above.

Remember: The law requires most providers to bill Medicare electronically and EDI access is crucial to that process. Protect your access and protect your patients' confidentiality by abiding by Medicare's privacy and security requirements.

If you have any questions regarding this issue, contact the EDI department of your carrier/intermediary at their toll-free number. If you bill for Medicare Part A services, including outpatient hospital services, that number may be found at

<http://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/downloads/MedicarePartAEDIHelpline.pdf> on the CMS website.

If you bill for Medicare Part B services, that number may be found at

<http://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/downloads/MedicarePartBEDIHelpline.pdf> on the CMS website.

Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.