

CMS EDI Enrollment Attestation Form 10164C

Entities seeking to acquire an Electronic Data Interchange (EDI) Trading Partner Identification Number (ID) to conduct Medicare billing transactions and/or that retrieve electronic reports are required to review, and, as appropriate, respond, agree, and/or attest to the assertions contained in CMS Form 10164C.

A. Assurances

1. With respect to any and all aspects of my access to; maintenance, use, and disclosure of; and return and/or destruction of Centers for Medicare & Medicaid Services (CMS) data, I will abide by all applicable federal laws, regulations, and guidance governing access to, use, and disclosure, of CMS data, including, but not limited to, all provisions pertaining to Protected Health Information (PHI) as defined in 45 CFR § 160.103 and Personally Identifiable Information (PII) as defined in OMB Memorandum M-17-12 (January 03, 2017). I understand that individuals or entities may be subject to administrative, civil, and/or criminal penalties or other consequences for failing to abide by such provisions.
2. I will abide by CMS's and its Authorized Representative's guidelines for testing the transmission of Health Insurance Portability and Accountability Act of 1996 (HIPAA) transactions through the EDI front-end processing systems to ensure the accuracy, timeliness, completeness, and security to be approved for submission of inbound HIPAA standard transactions, in accordance with this Agreement.
3. I will ensure the information I submit in each EDI transaction is timely, complete, accurate, and secure, and I will take precautions to prevent unauthorized access to the Medicare transmission and processing systems. I will ensure that each electronic transaction I submit to CMS conforms with the requirements applicable to the transaction.
4. I will only submit electronic transactions as an enrolled Medicare provider or supplier or as a HIPAA Business Associate working on behalf of a Medicare enrolled provider or supplier serving enrolled Medicare beneficiaries. As a HIPAA Business Associate, I agree to notify the CMS Authorized Representative(s) within 30 days if my relationship with a Medicare enrolled provider or supplier ends or changes as required by the EDI Rules of Behavior in Section B of this form. If I am a Business Associate, I agree to provide current information about the providers or suppliers for whom I submit transactions pursuant to the EDI Rules of Behavior, referenced below in section B. I understand and agree that CMS and/or CMS Authorized

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

Representative(s) reserves the right to confirm the status of a Business Associate relationship directly with a Medicare enrolled provider or supplier.

5. I will comply with the EDI Rules of Behavior, referenced below in section B of this form, and include the EDI Rules of Behavior from section B in my Business Associate contracts.
6. I understand this form constitutes an agreement that takes effect and is binding when signed by an authorized, or delegated, official of my organization.
7. Notwithstanding any expiration or termination of this agreement, I understand that my obligation survives to ensure the privacy and security of PHI and PII, to protect the confidentiality of CMS proprietary information, and to comply with federal and state laws and regulations that apply to this information.
8. I attest any offshore (any location outside of the United States (U.S.) and U.S. territories where U.S. law is non-binding) organization performing Medicare work directly, or indirectly on behalf of my organization, adheres to all terms specified in all sections of this document (Sections A. B. C.) and that I bear legal, financial, and any other responsibility in the event of any failure in this respect. I will avoid transmitting or storing sensitive data (PHI and PII) through countries listed on the State Department's Countries of Concern [website](#). If I do not perform any Medicare work offshore directly, or indirectly employ any offshore labor, I will mark this assurance as 'Not Applicable.' [☐] Not Applicable

B. EDI Rules of Behavior

The EDI Rules of Behavior explain your responsibilities as an EDI Trading Partner, and you must acknowledge that you understand and will comply with the EDI Rules of Behavior to obtain a Trading Partner ID.

1. My organization's security controls are, at a minimum, sufficient to ensure that every electronic transaction and response to/from CMS is associated with or can be traced back to a Medicare provider, supplier, or other user.
2. My organization will only release PHI/PII data to enrolled Medicare providers or suppliers with a Medicare EDI enrollment or their authorized HIPAA Business Associates to submit and receive accurate Medicare claim transactions.
3. My organization will include the EDI Rules of Behavior form in my other Business Associate contracts.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

4. My organization will cooperate with CMS or its agents and provide any information necessary to assist an investigation arising from a privacy or security concern with a transaction.
5. My organization will disclose any offshore arrangements to the entity that connects to CMS and/or CMS Authorized Representative(s) for their CMS Trading Partner Agreement.
6. My organization will not manipulate or obscure the originating IP address.
7. My organization will inform [CMS](#) and/or CMS Authorized Representative(s) within one hour upon suspicion or actual knowledge of misuse of PII and/or PHI, including unauthorized access, use, or disclosure. Information to make a report is located at the following website, [CMS.gov - Reporting Fraud](#).
8. My organization will not disclose, lend, or otherwise transfer EDI Trading Partner IDs and/or passwords or other credentials.
9. My organization will not browse or use CMS and/or CMS Authorized Representative(s) data for personal gain or unauthorized or illegal purposes.

☐ I acknowledge that I have read, understand, and will abide by the EDI Trading Partner Rules of Behavior. I have also shared the EDI Rules of Behavior with my Business Associates and will enforce compliance.

C. Cybersecurity Attestations

Health Care Clearinghouses, Billing Services, and other third-party organizations must complete section C.1. Medicare enrolled providers or suppliers must complete section C.2.

1. Required for Health Care Clearinghouses, Billing Services and any other third -party organizations requesting an EDI Trading Partner ID.

Instructions: The following section should be completed by, or in immediate consultation with, your organization's security team, security coordinator/liaison, and/or Chief Information Security Officer (CISO). A selection is required for each attestation below.

Note: For questions 13 and 14, a Billing Continuity Plan is defined as the approach to submit claims and/or receive Electronic Remittance Advice (ERA) in the event of a disruption in your billing service.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

#	Attestation	Selection
1.	I attest that my organization's cybersecurity controls comply with HIPAA's privacy and security rules and the National Institute of Standards and Technology (NIST) or other comparable security frameworks.	Agree / Disagree [] []
2.	I attest that my organization's HIPAA Business Associates have attested to compliance with HIPAA's privacy and security rules, as well as the NIST or other comparable security frameworks.	Agree / Disagree [] []
3.	I attest that my organization utilizes identity control & authentication management to protect sensitive data and prevent unauthorized access, so that each individual with access to my organization's systems and network has a unique user identification, password, and is required to utilize multifactor authentication (MFA).	Agree / Disagree [] []
4.	I attest that my organization has implemented MFA for all critical functions that are public/internet facing.	Agree / Disagree [] []
5.	I attest that my organization is using hardware and software that is supported by a vendor with secure configurations and conducts regular maintenance such as patching or updates.	Agree / Disagree [] []
6.	I attest that my organization has had an annual independent information system security audit, that satisfies 45 CFR 164.312(b) and any associated implementation specifications or guidance, in the past 365 days.	Agree / Disagree [] []
7.	I attest that, upon request, my organization will provide evidence of the findings of the annual independent information system security audit. Expectations for this request would be an executive summary of the audit findings (i.e. number of High, Medium, and Low findings).	Agree / Disagree [] []
8.	I attest that my company encrypts all sensitive data (e.g. PHI / PII) at rest (stored on devices or systems).	Agree / Disagree [] []
9.	I attest that my company encrypts all sensitive data (e.g. PHI / PII) in transit.	Agree / Disagree [] []

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

#	Attestation	Selection
10.	<p>I attest that my organization's systems and network are scanned for vulnerabilities on a regular basis.</p> <ul style="list-style-type: none"> If agree, how often are your systems and network scanned by security software? 	<p>Agree / Disagree <input type="checkbox"/> <input type="checkbox"/></p> <p>One choice is required if Agree is selected: <input type="checkbox"/> At least every 72 hours <input type="checkbox"/> Every week <input type="checkbox"/> Every month <input type="checkbox"/> More than a month</p>
11.	<p>I attest that my organization requires a penetration test of mission critical systems.</p> <ul style="list-style-type: none"> If agree, how often are your mission critical systems tested? 	<p>Agree / Disagree <input type="checkbox"/> <input type="checkbox"/></p> <p>One choice is required if Agree is selected: <input type="checkbox"/> At least annually <input type="checkbox"/> Every two years <input type="checkbox"/> Every three years <input type="checkbox"/> At least once every 5 years or Ad Hoc</p>
12.	<p>I attest that my organization utilizes a documented and industry-recognized risk management framework (RMF), such as NIST 800-53 Security and Privacy Controls and other comparable security frameworks for Information Systems and Organizations and/or the CMS Risk Management Handbook (RMH) Chapter 14 Risk Assessment that identifies risks, likelihood, severity, and corrective actions.</p>	<p>Agree / Disagree <input type="checkbox"/> <input type="checkbox"/></p>

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

#	Attestation	Selection
13.	<p>I attest that my company has a Billing Continuity Plan in place in the event of a disruption to operations.</p> <ul style="list-style-type: none"> • If agree, how quickly can your Billing Continuity Plan be executed to fully resume operations? • If disagree, will you be creating a Billing Continuity Plan? 	<p>Agree / Disagree [] []</p> <p>One choice is required if Agree is selected: [] Within 24 hours [] Within 48 hours [] Within 72 hours [] Longer than 72 hours</p> <p>One choice is required if Disagree is selected: [] Yes, within the next year [] No or longer than one year</p>
14.	<p>I attest that my company has successfully tested our Billing Continuity Plan.</p> <ul style="list-style-type: none"> • If agree, when was your last test conducted? 	<p>Agree / Disagree [] []</p> <p>One choice is required if Agree is selected: [] Within last 365 days [] Longer than 365 days</p>

2. Required for Medicare providers or suppliers requesting an EDI Trading Partner ID:

Instructions: The following section should be completed by, or in immediate consultation with, your organization's security team, security coordinator/liaison, and/or Chief Information Security Officer (CISO). A selection is required for each attestation below.

Note: For question 12, a Billing Continuity Plan is defined as the approach to submit claims and/or receive Electronic Remittance Advice (ERA) in the event of a disruption in your billing service.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

*Estimated number of employees in your Organization: ☐ <10 ☐ <50 ☐ <100 ☐ 100 or more

*Estimated volume of claims submitted per month: ☐ <10 ☐ <100 ☐ < 500 ☐ Greater than 1000

#	Attestation	Selection
1.	I attest that my organization's cybersecurity controls are in compliance with HIPAA's privacy and security rules, as well as the National Institute of Standards and Technology (NIST) or other comparable security frameworks.	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2.	I attest that my organization's HIPAA Business Associates have attested to compliance with HIPAA's privacy, security rules, as well as the NIST or other comparable security frameworks.	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3.	I attest that my organization utilizes identity control & authentication management to protect sensitive data and prevent unauthorized access, so that each individual with access to my organization's systems and network has a unique user id, password, and multifactor authentication (MFA).	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4.	I attest that my organization has implemented MFA for all critical functions that are public/internet facing.	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5.	I attest that my organization is using hardware and software that is supported by a vendor with secure configurations and conducts regular maintenance such as patching or updates.	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6.	I attest that my organization has had an annual independent information system security audit that, satisfies 45 CFR 164.312(b) and any associated implementation specifications or guidance, in the past 365 days.	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7.	I attest that, upon request, my organization will provide evidence of the findings of the annual independent information system security audit. Expectations for this request would be an executive summary of the audit findings (i.e. number of High, Medium, and Low findings).	Agree / Disagree / Unknown <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

#	Attestation	Selection
8.	I attest that my company encrypts all sensitive data (e.g. PHI / PII) at rest (stored on devices or systems).	Agree / Disagree / Unknown [] [] []
9.	I attest that my company encrypts all sensitive data (e.g. PHI / PII) in transit.	Agree / Disagree / Unknown [] [] []
10.	I attest that my organization's systems and network are scanned for vulnerabilities on a regular basis. <ul style="list-style-type: none"> If agree, how often are your systems and network scanned by security software? 	Agree / Disagree / Unknown [] [] [] One choice is required if Agree is selected: [] At least every 72 hours [] Every week [] Every month [] More than a month
11.	I attest that my organization requires a penetration test of mission critical systems. <ul style="list-style-type: none"> If agree, how often are your mission critical systems tested? 	Agree / Disagree / Unknown [] [] [] One choice is required if Agree is selected: [] At least annually [] Every two years [] Every three years [] At least once every 5 years or Ad Hoc
12.	I attest that my organization utilizes a documented and industry-recognized risk management framework (RMF), such as NIST 800-53 Security and Privacy Controls and other comparable security frameworks for Information Systems and Organizations and/or the CMS Risk Management Handbook (RMH) Chapter 14 Risk Assessment that identifies risks, likelihood, severity, and corrective actions.	Agree / Disagree / Unknown [] [] []

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850

#	Attestation	Selection
13.	I attest that my company or the entity which submits my claims and retrieves my Electronic Remittance Advice has a Billing Continuity Plan in place in the event of a disruption to operations.	Agree / Disagree / Unknown [] [] []

D. Authorized Signature:

By signing the below, my organization confirms that it has read and agrees to the CMS cybersecurity assurances and EDI Rules of Behavior for conducting electronic Medicare billing transactions.

All fields marked with * are required and must be completed.

Name of Organization*:

Trading Partner/Submitter ID (Optional): _____

Provider Transaction Access Number (PTAN) *: _____

National Provider Identifier (NPI)*: _____

The person listed below must be authorized to bind your organization as a Trading Partner. By completing and signing the section below, you agree that your organization will comply with the provisions of this Agreement.

Name of Approver for Organization*: _____

Signature of Approver for Organization*: _____

Date*: _____

Email Address*: _____

Telephone Number*: _____

Reminder: This form will also be required for Medicare EDI recertification.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0983. The time required to complete this information collection is estimated to average (hours) (minutes) per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850