

Centers for Medicare & Medicaid Services esMD HII Agreement

This HII – CMS esMD Agreement, hereafter referred to as “Agreement”, is made as of _____ to become effective on _____ for a validity period of **12 months** between _____ organization as the Health Information Handler (HII) and the Centers for Medicare & Medicaid Services (CMS), hereafter referred to as “both parties”, for secure exchange of health information using the Electronic Submission of Medical Documentation (esMD) system and all its affiliated systems. This agreement needs to be signed no later than **December 31, 2023**.

The HII, also known as the Submitter, intends to submit medical documentation and conduct Prior Authorization Review and Response transactions with CMS in electronic form. Both parties acknowledge and agree that the privacy and security of data held by or exchanged between them is of utmost priority. Each party agrees to take all steps reasonably necessary to ensure that all electronic transactions between them conform to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated thereunder. Unless defined herein, all terms have the same meaning as in the regulations promulgated to implement the Administrative Simplification provisions of HIPAA at 45 CFR Parts 160-164. All Cross-Enterprise Document Reliable Interchange (XDR) electronic transactions are subject to the same privacy and security requirements.

This Agreement in no way infringes on the pre-established agreement between the HII and their represented healthcare provider(s) and/or supplier(s).

I. REQUIREMENTS

CMS is committed to maintaining the integrity and security of health care data in accordance with applicable laws and regulations. Disclosure of Medicare beneficiary data is restricted under the provisions of the Privacy Act of 1974 (Privacy Act) and HIPAA. The esMD transaction is to be used for conducting Medicare and Medicaid businesses only. In its administration of the Medicare Fee-For-Service (FFS) and Medicaid programs, CMS is a covered entity under the HIPAA rules. This Agreement serves to identify entities external to CMS that will exchange HIPAA compliant electronic transactions with CMS software applications. The esMD system supports the prior authorization request/response in the standard transaction format (ANSI ASC X12N/005010X217 (278)). The information collected by the esMD system will enable CMS and the HII to establish connectivity, define the data exchange requirements, and stipulate the responsibilities of the entities receiving CMS-supplied information.

The requirements for connectivity and health data exchange between CMS and the HII are for the express purpose of enabling the HII represented provider(s) and/or supplier(s) to submit documentation supporting Medicare/Medicaid claims processing, via the HII Gateways, owned by the HIIs, through the esMD System, owned by CMS, to the various Review Contractors (RCs) contracted by CMS to conduct medical reviews. CMS sends acknowledgements and messages

(Including error messages) about HIIH-submitted medical documentation, and RCs' decision results for Prior Authorization/Pre-Claim Review Requests and ADR Responses to the HIIH's Gateway. HIIH access is as approved and directed by an appropriate authority at CMS following the esMD on-boarding process. The expected benefit is to expedite and confirm the submission and review of medical documentation to support claims processing and to expedite decisions on the Prior Authorization Requests for services under several Prior Authorization programs and Pre-Claim Review demonstrations initiated by CMS.

The following requirements are applicable to all HIIHs:

1. All HIIHs shall maintain an active signed agreement with each of their respective providers and/or suppliers that they represent. These agreements shall require HIPAA compliance. If a future audit occurs, the HIIHs shall either provide access to view those agreement(s) or provide evidence of having them.
2. All HIIHs are required to renew this Agreement and their Transport Layer Security (TLS) Certificates before their expiry, with at least 30 days' notice to CMS.
3. HIIHs shall safeguard all Protected Health Information (PHI) and Personally Identifiable Information (PII).
4. HIIHs shall notify CMS within reasonable time of any significant HIIH organizational change that affects this agreement.
5. HIIHs are required to update their contact information and keep it current at all times for the CMS esMD Support team to be able to reach them when needed.
6. All HIIHs shall support any Line of Business that esMD supports in the XDR format and/or Prior Authorization program/Pre-Claim Review demonstration services in ASC X12N/005010X217 (278) format. Paired services such as Prior Authorization Requests and Responses and Prior Authorization Decision Letters (PADL); Electronic Medical Documentation Requests (eMDR), ADR/eMDR Responses and Review Result Letters (RRL) (only if supported by that particular RC) shall be supported in conjunction. Prior Authorization Decision Letters and Review Result Letters shall be supported in the XDR and/or JSON format.
7. HIIHs' Gateways are required to send receipt acknowledgements for RC Pick-Up Notices and Decision Responses, process messages from esMD, and follow-up on all error messages from esMD.
8. HIIHs are required to participate in the monthly HIIH Calls with the CMS esMD team and quarterly Community Calls with the RCs and the CMS esMD Team.
9. HIIHs are required to participate in User Acceptance Testing (UAT) and attend all UAT kick-off and status meetings. If there are new lines of business being implemented and tested that are not a part of the HIIHs business operations, then Regression testing for current lines of business shall be performed.
10. No later than December 31st, each HIIH is required to have a separate test instance to interact with the esMD Validation environment; it is not acceptable to send test transactions to the Production environment.

II. SYSTEM SECURITY CONSIDERATIONS

- **General Information/Data Description:** The connectivity and health information exchange between the esMD system, owned by CMS, and the HIIH Gateway, owned by the HIIH, is a two – way path. The exchanges of data between esMD and the HIIH's system are accomplished using the security standards and protocols defined by CMS and the Sequoia Project (formerly known as the Healthway and originally as the Nationwide Health Information Network [NHIN]) via the Internet.
- **Services Offered:** CMS does not offer end user (User Interface) services to the HIIH's users. This system-to-system connection allows medical documentation data, submitted by providers to the HIIH, and HIIH acknowledgements of notices/decisions, Prior Authorization Decision Letters and Review Result Letters to be delivered to the RCs and allows esMD to send to the HIIH Gateway; 1) error messages generated by esMD or the RCs, 2) transfer of documentation to RCs folder, 3) receipt of documentation notices from the RCs, 4) Review Results Letters from the RCs, and 5) decision responses and Prior Authorization Decision Letters from the RCs for Prior Authorization Requests and Pre-Claim Reviews submitted by the HIIH.
- **Data Sensitivity:** The sensitivity of data exchanged between CMS and the HIIH is Sensitive-But-Unclassified.
- **User Community:** CMS users include systems developers/maintainers and operational support personnel with limited access to the data elements and no access to the supporting documentation received from the HIIHs, and RCs who are the targeted users of the data and documentation submitted by the HIIHs. The HIIH system and the esMD system must each provide protection for the data and documentation submitted by the providers/suppliers and the acknowledgements and responses submitted by the RCs:
 - The submitted data and documentation must remain available for the authorized users of each system according to their agreed policies;
 - The submitted data and documentation must be protected from unauthorized alteration or loss; and
 - The submitted data and documentation must be protected from unauthorized disclosure.
- **Information Exchange Security:** The security of the information being passed through this two-way connection is protected through the use of FIPS 140-2 compliant TLS Certificate and encryption mechanisms at the HIIH and CMS; this includes the use of Entrust certificates. The connections at the CMS end are located within controlled access facilities, guarded 24 hours a day. There are no individual users of the CMS esMD Gateway. The only individual users accessing the HIIH-submitted data are the RC users who download the transactions with their attached supporting documentation. The individual RC users and the esMD System access the data only through the systems security software inherent to the operating system. All individual RC user access is controlled by authentication methods to validate the approved users. There are a maximum of four users per RC. The connections at the HIIH end are located within the HIIH datacenter; access is granted only to HIIH – authorized users. Access to the esMD Gateway is available only through a system-to-system connection and there are no individual user accesses of the esMD Gateway available at the HIIH end.

- **Authority:** Authority for this Agreement is based on, but not limited to, the following:
 - Federal Information Security Management Act of 2002 (FISMA);
 - OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems;
 - 18 United States Code U.S.C. 641 Criminal Code: Public Money, Property or Records;
 - 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information;
 - Privacy Act of 1974, 5 U.S.C. § 552a; and
 - Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-191.

- **Trusted Behavior Expectations:** CMS' esMD System is expected to protect the HHI's Gateway, and the HHI's system and users are expected to protect CMS's esMD System, in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710).

- **Formal Security Policy:** Policy documents that govern the protection of the data are dictated by CMS, and located at <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/InformationSecurity-Library.html>

- **Incident Reporting:** The party discovering a security incident will report it in accordance with its incident reporting procedures. In the case of the HHI, any security incident will also be reported to the esMD Service Desk and will be escalated to the appropriate party. Policy governing the reporting of Security Incidents is located at <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html>

- **Audit Trail Responsibilities:** Both parties are responsible for supporting esMD audit process and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year. Audit events and audit exceptions recorded in the esMD database will be retained for seven (7) years.

III. AUTHORIZED USES

Medicare and Medicaid data are only to be used for Medicare and Medicaid business done on behalf of Medicare FFS providers and Medicaid providers, including submitting accurate medical documentation or requesting prior authorization for specific services. HHIs cannot electronically store or reuse Medicare and Medicaid beneficiary Protected Health Information (PHI) obtained from esMD, except for the following purposes, when expressly authorized by CMS:

- To maintain an historical account of processing activity.
- In accordance with procedures (e.g., routine system backups) to support data restoration in the event of a disaster.
- To store in submitting programs for the benefit of the end user.

IV. SYSTEM INTEGRITY

CMS monitors esMD transactions. Submitters demonstrating behavior that constitutes improper use of the data may be suspended, placed on a corrective action plan (CAP) or, when appropriate, be referred for investigation. Civil and/or criminal enforcement may be pursued where appropriate.

1. HIPAA Violation

The U.S. Department of Health and Human Services (HHS) may impose civil money penalties on a covered entity of up to \$50,000 per failure to comply with a Privacy Rule requirement, up to an annual calendar year limit of \$1,500,000 for multiple violations of the identical Privacy Rule requirement. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces criminal penalties ranging from \$50,000 and up to one-year imprisonment to up to \$250,000 and up to ten years imprisonment, in circumstances where the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal enforcement is conducted by the Department of Justice.

2. Civil False Claims Act Violation and Criminal Violations

The False Claims Act, 31 U.S.C. §§ 3729-3733, provides that one who knowingly submits, or causes another person or entity to submit, false claims for payment of government funds is liable for three times the government's damages plus civil penalties of \$5,500 to \$11,000 per false claim.

Various federal criminal provisions authorize imposition of criminal penalties, including fines and imprisonment, against individuals who, with respect to Government or health care benefit programs, engage in conduct including, but not limited to, falsifying or concealing a material fact or making a materially false, fictitious, or fraudulent statement.

V. ASSURANCES

Provision by CMS of access to the esMD system, is subject to Submitter's assurances as set forth below. Access to the esMD system may be terminated by CMS in the event that Submitter has not complied with one or more of the assurances hereafter provided by Submitter.

In consideration of the foregoing, and in order to obtain access to the esMD system, the Submitter hereby agrees and assures as follows:

All Submitters (HIHs)

1. Submitter agrees to abide by all applicable federal laws, regulations, and guidance governing access to, and use and disclosure of, CMS data, Protected Health Information (PHI) as defined in 45 CFR §160.103, and Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 (May 22, 2007) and understands that individuals or entities may be subject to civil and/or criminal penalties for failing to abide by such provisions.
2. In cases where CMS reasonably suspects technical problems, before initiating a transmission to esMD, and thereafter through the term of this Agreement, the HIH will

reasonably cooperate with CMS and any contractors representing CMS in testing of the transmission and processing systems used in connection with esMD as deemed appropriate to ensure the accuracy, timeliness, completeness, and security of each data transmission.

3. Submitter will take reasonable care to ensure that the information submitted in each electronic transaction is submitted timely after end user authorization (as applicable), transmits all submitted documentation completely, accurately, and securely. Submitter will take reasonable precautions to prevent unauthorized access of the party's transmission and processing systems. The Submitter will ensure that each electronic transaction submitted to CMS conforms with the requirements applicable to the transaction.
4. This Agreement shall take effect and be binding on the HHH and CMS when signed by the HHH and reviewed and signed by an authorized CMS representative.
5. Termination or expiration of this Agreement or any other agreement or contract between the parties does not relieve either party of its obligations under this Agreement and under federal and state laws and regulations pertaining to the privacy and security of PHI and PII, nor its obligations regarding the confidentiality of CMS proprietary information.

The Authorized Representative whose name is supplied below is authorized to bind the HHH, as esMD Submitter, to the undertakings of this Agreement. By completing the section below, you are agreeing that your organization will be in compliance with the provisions of this Agreement.

HHH Authorized Representative Signature

Title

Printed Name of HHH Authorized Signer

Date Signed

E-Mail Address

Telephone Number

CMS Official Signature

Title

Printed Name of CMS Official Signer

Date Signed