MINNESOTA DHS ELECTRONIC DATA INTERCHANGE TRADING PARTNER ADDENDUM TO PROVIDER AGREEMENT FOR MN–ITS

This Agreement is an addendum to the existing Provider Agreement between the Minnesota Department of Human Services (DHS) and the enrolled health care provider identified in this agreement (provider). By entering into this Provider Agreement, you are acknowledging that you are the provider or an agent of the provider, acting as an Electronic Data Interchange (EDI) Trading Partner, and agree, on behalf of the provider, to the following service descriptions, terms and conditions.

Definitions

Electronic Data Interchange (EDI) means the computer-to-computer exchange of traditional business documents using structured industry standards and formats which can be easily processed by a computer application. For this Agreement, the sole vehicle for EDI is the MN–ITS application.

EDI Trading Partner means an organization or individual that transmits heath care transactions to and from the Minnesota Health Care Programs (MHCP) administered by DHS, either as the provider or as an agent on behalf of the provider. It includes billing agents, eligibility verification vendors, Medicare billing intermediaries, billing intermediaries, and clearinghouses.

Minnesota Health Care Programs (MHCP) means the publicly subsidized health care programs administered by DHS, including Medical Assistance (MA) and MinnesotaCare.

MN–ITS (Minnesota Information Transfer System) is a web-based, Health Information Portability and Accountability Act (HIPAA)-compliant billing and inquiry system for claims submission and other health care transactions with MHCP. MN–ITS consists of both an interactive component (direct data entry), and a batch component, which are X12 compliant.

Privacy Incident means violation of the Minnesota Government Data Practices Act (MGDPA) or the HIPAA privacy rule (Code of Federal Regulations, title 45, part 164, subpart E). It includes violation of other privacy laws and regulations, including, but not limited to, improper or unauthorized use or disclosure of protected information, and incidents in which the confidentiality of the information maintained by it has been breached.

Protected Health Information (PHI) means any information, including demographic information collected from an individual, that is:

- created or received by a health care provider, health plan, employer, billing agent, eligibility verification vendor, Medicare billing intermediary, or health care clearinghouse; and
- related to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual, or reasonably can be a basis to identify the individual (Code of Federal Regulations, title 45, part 160.103).

Protected Information includes:

- private data (as defined in Minnesota Statutes, 13.02, subdivision 12),
- confidential data (as defined by Minnesota Statutes, 13.02, subdivision 3),
- welfare data (as governed by Minnesota Statutes, 13.46),
- medical records (as governed by Minnesota Statutes, 13.384 and 144.291 – 144.298),
- chemical health records (as governed by Unites States Code, title 42, section 290dd-2 and Code of Federal Regulations, title 42, sections 2.1 – 2.67), and
- Protected Health Information.

Provider means an organization or individual that has enrolled with DHS to provide health services to members of MHCP and is eligible to receive payment from DHS for those services.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Transactions means the information or data transmitted through MN–ITS between DHS and providers and EDI Trading Partners to carry out financial, reporting, contracting, or administrative activities related to health care. The term "transaction" includes, but is not limited to, health care claims, remittance advices, eligibility, and as otherwise set out in Code of Federal Regulations, title 45, section 160.103.

Terms and Conditions

EDI Trading Partner Duties. EDI trading partner agrees to:

1. Submit claims only on its own behalf or on behalf of those providers who have given written authorization to the EDI trading partner. Such authorizations will be maintained by both the EDI trading partner and the provider during the term of this agreement.
2. Accept and be bound by the terms and conditions of DHS' Provider Agreement.
3. Maintain a record of all claims submitted for five years, or the duration of contested case proceedings, whichever is longer.
4. Not change any definition, data condition, or use of a data element in the transmission of information in standard transactions.
5. Not add any data elements or segments to the maximum defined data set for the transmission of standard transactions.
6. Submit test files to DHS when using batch transactions, if it is a new EDI trading partner.
7. Use the X12 or NCPDP version and accompanying Companion Guides for batch EDI trading partners required by state and federal law.
8. Not use any code or data elements that are either marked "not used" in the standard's implementation specifications or are not in the standard's implementation specifications for the transmission of information in standard transactions.
9. Not change the meaning or intent of any of the standard's implementation specifications for the transmission of information in standard transactions.
10. Participate in testing modifications if DHS or others request an exception from the uses of a standard in the transaction standards.
11. Test all business rules appropriate to each provider type and specialty for which it provides EDI services.
12. Correct transaction errors or deficiencies identified by DHS or by a provider.
13. Use the latest versions of transaction standards when the federal or state government enacts or changes them.
14. Keep available for use code sets being processed or used in this agreement for at least the current billing period and any appeal period, if applicable.

15. Provide DHS, the Minnesota Attorney General's Medicaid Fraud Control Unit (MFCU), the United States Secretary of Health and Human Services (DHHS), and their designees, access to audit and confirm for any purpose information submitted to the EDI trading partner by providers. Any incorrect MHCP payments that are discovered by an audit will be adjusted according to the applicable provisions of state and federal law. The EDI trading partner understands that payment of claims will be from federal and state funds, and that any falsification or concealment of a material fact may be prosecuted under federal and state laws.
16. Ensure proper handling and safeguarding by its employees, subcontractors, and authorized agents of protected information collected, created, used, maintained, or disclosed on behalf of DHS. This responsibility includes:
    a. Ensure that employees and agents of the EDI trading partner comply with and are properly trained regarding:
        - The Minnesota Government Data Practices Act (MGDPA), Minnesota Statutes, chapter 13, in particular section 13.46 (welfare data);
        - The Minnesota Medical Records Act, Minnesota Statutes, 144.291 – 144.298;
        - The Health Insurance Portability Accountability Act (HIPAA), including but not limited to the requirements of the privacy rule and the security regulations, Code of Federal Regulations, title 45, parts 160 and 164.
        - The False Claims Act, United States Code, title 31, sections 3729 – 3733.
        - Applicable federal law and regulations that govern the use and disclosure of substance abuse treatment records, Unites States Code, title 42 , section 290dd-2 and Code of Federal Regulations, title 42, sections 2.1 – 2.67; and
        - Any other applicable state and federal statutes, rules and regulations affecting the collection, storage, use and dissemination of private or confidential information.
    b. Ensure that, consistent with the preceding laws, the EDI trading partner's employees, subcontractors, and authorized agents:
        - Not use or further disclose protected information created, collected, received, stored, used, maintained or disseminated in the course or performance of this agreement other than as necessary to perform its obligations under this agreement, or as required by law, either during the period of this agreement or hereafter. (*See* 45 Code of Federal Regulations, sections 164.502(b) and 164.514(d), and Minnesota Statutes, 13.05, subdivision 3.)
        - Use appropriate administrative, physical, and technical safeguards to prevent use or disclosure of the protected information, other than as provided for by this agreement and to ensure the confidentiality, integrity, and availability of any electronic PHI that it creates, receives, maintains, or transmits on behalf of DHS. The EDI trading partner will not transmit PHI over the internet or any other unsecure or open communications channel unless such information is encrypted or otherwise safeguarded using procedures no less stringent than those described in the Code of Federal Regulations, title 45 CFR, section164.312. (MN–ITS is a secure, HIPAA-complaint web application.) If the EDI trading partner stores or maintains PHI in encrypted form, the EDI trading partner shall, at DHS' request, promptly provide DHS with the key or keys to decrypt such information. The EDI trading partner shall not forward previously encrypted data to any other party.
        - Mitigate to the extent practicable, any harmful effects known to the EDI trading partner of a use, disclosure, or breach of security with respect to protected information by the EDI trading partner in violation of this agreement.
        - Report to DHS any privacy incident or security incident or any other breach of the security of data covered under the MGDPA of which it becomes aware.
        - Make the required notifications upon discovery of a breach, as defined in the Code of Federal Regulations, title 45, section 164.402, of unsecured PHI to DHS, to each individual whose unsecured PHI has been breached, and, when the breach involves the unsecured PHI of more than 500 residents, to the media of a state or jurisdiction. (See the Code of Federal Regulations, title 45, sections 164.400 – 164.414.)

Ambiguity. The parties agree that any ambiguity in this Provider Agreement shall be resolved to permit DHS to comply with HIPAA, MGDPA, and other applicable state and federal statutes, rules, and regulations affecting the collection, storage, use and dissemination of private or confidential information and other state and federal laws and regulations.

Monitoring. The EDI trading partner acknowledges that DHS may monitor any and all activity related to the use of the MN–ITS system to ensure compliance with this agreement and pertinent state and federal laws and as otherwise allowed by Minnesota Statutes, 13.15, subdivision 4.

Termination. DHS may terminate this Provider Agreement at any time with or without cause. Upon termination of this agreement, the EDI trading partner shall continue to extend to all of the protected information provided by DHS to the EDI trading partner, or provided on behalf of DHS to the EDI trading partner, that the EDI Trading Partner still maintains in any form, including information that is in the hands of the subcontractors and agents of the EDI trading partner, all of the protections of this addendum and the Provider Agreement and to limit its further use and disclosure. The EDI trading partner must continue to maintain all other records of claims submitted for a minimum of five years, consistent with state law.

Liability. The EDI trading partner acknowledges that DHS will not be liable for any violation of any provision of the applicable data privacy and security laws that indirectly or directly arises out of, results from, or in any manner is attributable to actions of the EDI trading partner or its employees or agents. In addition, the EDI trading partner agrees to indemnify and hold DHS, its agents and employees, harmless for all claims arising out of, resulting from, or in any manner attributable to any violation by the EDI trading partner or its employees or agents, of any provision of the applicable data privacy and security laws, including legal fees and disbursements paid or incurred to enforce this provision of the contract.