CHAPTER 407
DEPARTMENT OF HUMAN SERVICES,
ADMINISTRATIVE SERVICES DIVISION AND DIRECTOR'S OFFICE

DIVISION 120
PROVIDER RULES

Electronic Data Transmission

407-120-0100
Definitions

The following definitions apply to OAR 407-120-0100 through 407-120-0200:

(1) "Access" means the ability or means necessary to read, write, modify, or communicate data or information or otherwise use any information system resource.

(2) "Agent" means a third party or organization that contracts with a provider, allied agency, or prepaid health plan (PHP) to perform designated services in order to facilitate a transaction or conduct other business functions on its behalf. Agents include billing agents, claims clearinghouses, vendors, billing services, service bureaus, and accounts receivable management firms. Agents may also be clinics, group practices, and facilities that submit billings on behalf of providers but the payment is made to a provider, including the following: an employer of a provider, if a provider is required as a condition of employment to turn over his fees to the employer; the facility in which the service is provided, if a provider has a contract under which the facility submits the claim; or a foundation, plan, or similar organization operating an organized health care delivery system, if a provider has a contract under which the organization submits the claim. Agents may also include electronic data transmission submitters.

(3) "Allied Agency" means local and regional allied agencies and includes local mental health authority, community mental health programs, Oregon Youth Authority, Department of Corrections, local health departments, schools, education service districts, developmental disability service programs, area agencies on aging, federally recognized American Indian tribes, and other governmental agencies or regional authorities that have a contract (including an interagency, intergovernmental, or grant agreement, or an agreement with an American Indian tribe pursuant to ORS 190.110) with the Department to provide for the delivery of services to covered individuals and that request to conduct electronic data transactions in relation to the contract.

(4) "Clinic" means a group practice, facility, or organization that is an employer of a provider, if a provider is required as a condition of employment to turn over his fees to the employer; the facility in which the service is provided, if a provider has a contract under which the facility submits the claim; or a foundation, plan, or similar organization operating an organized health care delivery system, if a provider has a contract under

which the organization submits the claim; and the group practice, facility, or organization is enrolled with the Department, and payments are made to the group practice, facility, or organization. If the entity solely submits billings on behalf of providers and payments are made to each provider, then the entity is an agent.

(5) "Confidential Information" means information relating to covered individuals which is exchanged by and between the Department, a provider, PHP, clinic, allied agency, or agents for various business purposes, but which is protected from disclosure to unauthorized individuals or entities by applicable state and federal statutes such as ORS 344.600, 410.150, 411.320, 418.130, or the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and its implementing regulations. These statutes and regulations are collectively referred to as "Privacy Statutes and Regulations."

(6) "Contract" means a specific written agreement between the Department and a provider, PHP, clinic, or allied agency that provides or manages the provision of services, goods, or supplies to covered individuals and where the Department and a provider, PHP, clinic, or allied agency may exchange data. A contract specifically includes, without limitation, a Department provider enrollment agreement, fully capitated heath plan managed care contract, dental care organization managed care contract, mental health organization managed care contract, chemical dependency organization managed care contract, physician care organization managed care contract, a county financial assistance agreement, or any other applicable written agreement, interagency agreement, intergovernmental agreement, or grant agreement between the Department and a provider, PHP, clinic, or allied agency.

(7) "Covered Entity" means a health plan, health care clearing house, health care provider, or allied agency that transmits any health information in electronic form in connection with a transaction, including direct data entry (DDE), and who must comply with the National Provider Identifier (NPI) requirements of 45 CFR 162.402 through 162.414.

(8) "Covered Individual" means individuals who are eligible for payment of certain services or supplies provided to them or their eligible dependents by or through a provider, PHP, clinic, or allied agency under the terms of a contract applicable to a governmental program for which the Department processes or administers data transmissions.

(9) "Data" means a formalized representation of specific facts or concepts suitable for communication, interpretation, or processing by individuals or by automatic means.

(10) "Data Transmission" means the transfer or exchange of data between the Department and a web portal or electronic data interchange (EDI) submitter by means of an information system which is compatible for that purpose and includes without limitation, web portal, EDI, electronic remittance advice (ERA), or electronic media claims (EMC) transmissions.

(11) "Department" means the Department of Human Services.

(12) “Department Network and Information Systems” means the Department’s computer infrastructure that provides personal communications, confidential information, regional, wide area and local networks, and the internetworking of various types of networks on behalf of the Department.

(13) “Direct Data Entry (DDE)” means the process using dumb terminals or computer browser screens where data is directly keyed into a health plan’s computer by a provider or its agent, such as through the use of a web portal.

(14) “Electronic Data Interchange (EDI)” means the exchange of business documents from application to application in a federally mandated format or, if no federal standard has been promulgated, using bulk transmission processes and other formats as the Department designates for EDI transactions. For purposes of these rules (OAR 407-120-0100 through 407-120-0200), EDI does not include electronic transmission by web portal.

(15) “Electronic Data Interchange Submitter” means an individual or entity authorized to establish the electronic media connection with the Department to conduct an EDI transaction. An EDI submitter may be a trading partner or an agent of a trading partner.

(16) “Electronic Media” means electronic storage media including memory devices in computers or computer hard drives; any removable or transportable digital memory medium such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media includes but is not limited to the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Certain transmissions, including paper via facsimile and voice via telephone, are not considered transmissions by electronic media because the information being exchanged did not exist in electronic form before transmission.

(17) “Electronic Media Claims (EMC)” means an electronic media means of submitting claims or encounters for payment of services or supplies provided by a provider, PHP, clinic, or allied agency to a covered individual.

(18) “Electronic Remittance Advice (ERA)” means an electronic file in X12 format containing information pertaining to the disposition of a specific claim for payment of services or supplies rendered to covered individuals which are filed with the Department on behalf of covered individuals by providers, clinics, or allied agencies. The documents include, without limitation, the provider name and address, individual name, date of service, amount billed, amount paid, whether the claim was approved or denied, and if denied, the specific reason for the denial. For PHPs, the remittance advice file contains information on the adjudication status of encounter claims submitted.

(19) “Electronic Data Transaction (EDT)” means a transaction governed by the Health Insurance Portability and Accountability Act (HIPAA) transaction rule, conducted by either web portal or EDI.

(20) “Envelope” means a control structure in a mutually agreed upon format for the electronic interchange of one or more encoded data transmissions either sent or received by an EDI submitter or the Department.

(21) “HIPAA Transaction Rule” means the standards for electronic transactions at 45 CFR Part 160 and 162 (version in effect on January 1, 2008) adopted by the Department of Health and Human Services (DHHS) to implement the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq.

(22) “Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of an information system or information asset including but not limited to unauthorized disclosure of information, failure to protect user IDs, and theft of computer equipment using or storing Department information assets or confidential information.

(23) “Individual User Profile (IUP)” means Department forms used to authorize a user, identify their job assignment, and the required access to the Department’s network and information system. It generates a unique security access code used to access the Department’s network and information system.

(24) “Information Asset” means all information, also known as data, provided through the Department, regardless of the source, which requires measures for security and privacy of the information.

(25) “Information System” means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and trained personnel necessary for successful data transmission.

(26) “Lost or Indecipherable Transmission” means a data transmission which is never received by or cannot be processed to completion by the receiving party in the format or composition received because it is garbled or incomplete, regardless of how or why the message was rendered garbled or incomplete.

(27) “Mailbox” means the term used by the Department to indicate trading partner-specific locations on the Department’s secure file transfer protocol (SFTP) server to deposit and retrieve electronic data identified by a unique Department assigned trading partner number.

(28) “Password” means the alpha-numeric codes assigned to an EDI submitter by the Department for the purpose of allowing access to the Department’s information system, including the web portal, for the purpose of successfully executing data transmissions or

otherwise carrying out the express terms of a trading partner agreement or provider enrollment agreement and these rules.

(29) "Personal Identification Number (PIN)" means the alpha-numeric codes assigned to web portal submitters by the Department for the purpose of allowing access to the Department's information system, including the web portal, for the purpose of successfully executing DDE, data transmissions, or otherwise carrying out the express terms of a trading partner agreement, provider enrollment agreement, and these rules.

(30) "Prepaid Health Plan (PHP) or Plan" means a managed health care, dental care, chemical dependency, physician care organization, or mental health care organization that contracts with the Department on a case managed, prepaid, capitated basis under the Oregon Health Plan (OHP).

(31) "Provider" means an individual, facility, institution, corporate entity, or other organization which supplies or provides for the supply of services, goods or supplies to covered individuals pursuant to a contract, including but not limited to a provider enrollment agreement with the Department. A provider does not include billing providers as used in the Division of Medical Assistance (DMAP) general rules. DMAP billing providers are defined in these rules as agents, except for DMAP billing providers that are clinics.

(32) "Provider Enrollment Agreement" means an agreement between the Department and a provider for payment for the provision of covered services to covered individuals.

(33) "Registered Transaction" means each type of EDI transaction applicable to a trading partner that must be registered with the Department before it can be tested or approved for EDI transmission.

(34) "Security Access Codes" means the alpha-numeric codes assigned by the Department to the web portal submitter or EDI submitter for the purpose of allowing access to the Department's information system, including the web portal, to execute data transmissions or otherwise carry out the express terms of a trading partner agreement, provider enrollment agreement, and these rules. Security access codes may include passwords, PINs, or other codes.

(35) "Source Documents" means documents or electronic files containing underlying data which is or may be required as part of a data transmission with respect to a claim for payment of charges for medical services or supplies provided to a covered individual, or with respect to any other transaction. Examples of data contained within a specific source document include but are not limited to an individual's name and identification number, claim number, diagnosis code for the services provided, dates of service, service procedure description, applicable charges for the services provided, and a provider's, PHP's, clinic's, or allied agency's name, identification number, and signature.

(36) "Standard" means a rule, condition, or requirement describing the following information for products, systems, or practices:

(a) Classification of components;

(b) Specification of materials, performance, or operations; or

(c) Delineation of procedures.

(37) "Standards for Electronic Transactions" mean a transaction that complies with the applicable standard adopted by DHHS to implement standards for electronic transactions.

(38) "Transaction" means the exchange of data between the Department and a provider using web portal access or a trading partner using electronic media to carry out financial or administrative activities.

(39) "Trade Data Log" means the complete written summary of data and data transmissions exchanged between the Department and an EDI submitter during the period of time a trading partner agreement is in effect and includes but is not limited to sender and receiver information, date and time of transmission, and the general nature of the transmission.

(40) "Trading Partner" means a provider, PHP, clinic, or allied agency that has entered into a trading partner agreement with the Department in order to satisfy all or part of its obligations under a contract by means of EDI, ERA, or EMC, or any other mutually agreed means of electronic exchange or transfer of data.

(41) "Trading Partner Agreement (TPA)" means a specific written request by a provider, PHP, clinic, or allied agency to conduct EDI transactions that governs the terms and conditions for EDI transactions in the performance of obligations under a contract. A provider, PHP, clinic, or allied agency that has executed a TPA will be referred to as a trading partner in relation to those functions.

(42) "User" means any individual or entity authorized by the Department to access network and information systems or information assets.

(43) "User Identification Security (UIS)" means a control method required by the Department to ensure that only authorized users gain access to specified information assets. One method of control is the use of passwords and PINs with unique user identifications.

(44) "Web Portal" means a site on the World Wide Web that typically provides personalized capabilities to its visitors and a pathway to other content. It is designed to use distributed applications, different numbers, and types of middleware and hardware to provide services from a number of different sources.

(45) "Web Portal Submitter" means an individual or entity authorized to establish an electronic media connection with the Department to conduct a DDE transaction. A web portal submitter may be a provider or a provider's agent.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0110
Purpose

(1) These rules establish requirements applicable to providers, PHPs, and allied agencies that want to conduct electronic data transactions with the Department. These rules govern the conduct of all web portal or EDI transactions with the Department. These rules only apply to services or items that are paid for by the Department. If the service or item is paid for by a plan or an allied agency, these rules do not apply.

(2) These rules establish the Department's electronic data transaction requirements for purposes of the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d - 1320d-8, Public Law 104-191, sec. 262 and sec. 264, and the implementing standards for electronic transactions rules. Where a federal HIPAA standard has been adopted for an electronic data transaction, this rule implements and does not alter the federal standard.

(3) These rules establish procedures that must be followed by any provider, PHP, or allied agency in the event of a security or privacy incident, regardless of whether the incident is related to the use of an electronic data transaction.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0112
Scope and Sequence of Electronic Data Transmission Rules

(1) The Department communicates with and receives communications from its providers, PHPs, and allied agencies using a variety of methods appropriate to the services being provided, the nature of the entity providing the services, and constantly changing technology. These rules describe some of the basic ways that the Department will exchange data electronically. Additional details may be provided in the Department's access control rules, provider-specific rules, or the applicable contract documents.

(2) Access to eligibility information about covered individuals may occur using one or more of the following methods:

(a) Automated voice response, via a telephone;

(b) Web portal access;

(c) EDI submitter access; or

(d) Point of sale (POS) for pharmacy providers.

(3) Claims for which the Department is responsible for payment or encounter submissions made to the Department may occur using one or more of the following methods:

(a) Paper, using the form specified in the provider specific rules and supplemental billing guidance. Providers may submit paper claims, except that pharmacy providers are required to use the POS process for claims submission and plans are required to use the 837 electronic formats;

(b) Web portal access;

(c) EDI submitter access; or

(d) POS for pharmacy providers.

(4) Department informational updates, provider record updates, depository for plan reports, or EDT as specified by the Department for contract compliance.

(5) Other Department network and information system access is governed by specific program requirements, which may include but is not limited to IUP access. Affected providers, PHPs, and allied agencies will be separately instructed about the access and requirements. Incidents are subject to these rules.

(6) Providers and allied agencies that continue to use only paper formats for transactions are only subject to the confidentiality and security rule, OAR 407-120-0170.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0114
Provider Enrollment Agreement

(1) When a provider applies to enroll, the application form will include information about how to participate in the web portal for use of DDE and automated voice response (AVR) inquiries. The enrollment agreement will include a section describing the process that will permit the provider, once enrolled, to participate in DDE over the Internet using the secure Department web portal.

(2) When the provider number is issued by the Department, the provider will also receive two PINs: one that may be used to access the web portal and one that may be used for AVR.

(a) If the PINs are not activated within 60 days of issuance, the Department will initiate a process to inactivate the PIN. If the provider wants to use PIN-based access to the web portal or AVR after deactivation, the provider must submit an update form to obtain another PIN.

(b) Activating the PIN will require Internet access and the provider must supply security data that will be associated with the use of the PIN.

(c) Providers using the PIN are responsible for protecting the confidentiality and security of the PIN pursuant to OAR 407-120-0170.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0116
Web Portal Submitter

(1) Any provider activating their web portal access for web portal submission may be a web portal submitter. The provider will be referred to as the web portal submitter when functioning in that capacity, and shall be required to comply with these rules governing web portal submitters.

(2) The authorized signer of the provider enrollment agreement shall be the individual who is responsible for the provider's DDE claims submission process.

(a) If a provider submits their own claims directly, the provider will be referred to as the web portal submitter when functioning in that capacity and shall be required to comply with these rules governing web portal submitters.

(b) If a provider uses an agent or clinic to submit DDE claims using the Department's web portal, the agent or clinic will be referred to as the web portal submitter when functioning in that capacity and shall be required to comply with these rules governing web portal submitters.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0118
Conduct of Direct Data Entry Using Web Portal

(1) The web portal submitter is responsible for the conduct of the DDE transactions submitted on behalf of the provider, as follows:

(a) Accuracy of Web Portal Submissions. The web portal submitter must take reasonable care to ensure that data and DDE transmissions are timely, complete, accurate, and secure, and must take reasonable precautions to prevent

unauthorized access to the information system or the DDE transmission. The Department will not correct or modify an incorrect DDE transaction prior to processing. The transactions may be rejected and the web portal submitter will be notified of the rejection.

(b) Cost of Equipment. The web portal submitter and the Department must bear their own information system costs. The web portal submitter must, at their own expense, obtain access to Internet service that is compatible with and has the capacity for secure access to the Department's web portal. Web portal submitters must pay their own costs for all charges, including but not limited to charges for equipment, software and services, Internet connection and use time, terminals, connections, telephones, and modems. The Department is not responsible for providing technical assistance for access to or use of Internet web portal services or the processing of a DDE transaction.

(c) Format of DDE Transactions. The web portal submitter must send and receive all data transactions in the Department's approved format. Any attempt to modify or alter the DDE transaction format may result in denial of web portal access.

(d) Re-submissions. The web portal submitter must maintain source documents and back-up files or other means sufficient to re-create a data transmission in the event that re-creation becomes necessary for any purpose, within timeframes required by federal or state law, or by contractual agreement. Back ups, archives, or related files are subject to the terms of these rules to the same extent as the original data transmission.

(2) Security and Confidentiality. To protect security and confidentiality, web portal submitters must comply with the following:

(a) Refrain from copying, reverse engineering, disclosing, publishing, distributing, or altering any data or data transmissions, except as permitted by these rules or the contract, or use the same for any purpose other than that which the web portal submitter was specifically given access and authorization by the Department or the provider.

(b) Refrain from obtaining access by any means to any data or the Department's network and information system for any purpose other than that which the web portal submitter has received express authorization to receive access. If the web portal submitter receives data or data transmissions from the Department which are clearly not intended for the receipt of web portal submitter, the web portal submitter will immediately notify the Department and make arrangements to return or re-transmit the data or data transmission to the Department. After re-transmission, the web portal submitter must immediately delete the data contained in the data transmission from its information system.

(c) Install necessary security precautions to ensure the security of the DDE transmission or records relating to the information system of either the Department or the web portal submitter when the information system is not in active use by the web portal submitter.

(d) Protect and maintain, at all times, the confidentiality of security access codes issued by the Department. Security access codes are strictly confidential and specifically subject, without limitation, to all of the restrictions in OAR 407-120-0170. The Department may change the designated security access codes at any time and in any manner as the Department in its sole discretion considers necessary.

(e) Install, maintain, and use security measures for confidential information transmitted between a provider and the web portal submitter if a provider uses an agent or clinic as the web portal submitter.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0120
Registration Process – EDI Transactions

(1) The EDI transaction process is preferred by providers, PHPs, and allied agencies for conducting batch or real time transactions, rather than the individual data entry process used for DDE. EDI registration is an administrative process governed by these rules. The EDI registration process begins with the submission of a TPA by a provider, PHP, clinic, or allied agency, including all requirements and documentation required by these rules.

(2) Trading partners must be Department providers, PHPs, clinics, or allied agencies with a current Department contract. The Department will not accept a TPA from individuals or entities who do not have a current contract with the Department.

(a) The Department may receive and hold the TPA for individuals or entities that have submitted a provider enrollment agreement or other pending contract, subject to the satisfactory execution of the pending document.

(b) Termination, revocation, suspension, or expiration of the contract will result in the concurrent termination, revocation, suspension, or expiration of the TPA without any additional notice; except that the TPA will remain in effect to the extent necessary for a trading partner or the Department to complete obligations involving EDI under the contract for dates of service when the contract was in effect. Contracts that are periodically renewed or extended do not require renewal or extension of the TPA unless there is a lapse of time between contracts.

(c) Failure to identify a current Department contract during the registration process will result in a rejection of the TPA. The Department will verify that the contract

numbers identified by a provider, PHP, clinic, or allied agency are current contracts.

(d) If contract number or contract status changes, the trading partner must provide the Department with updated information within five business days of the change in contract status. If the Department determines that a valid contract no longer exists, the Department shall discontinue EDI transactions applicable for any time period in which the contract no longer exists; except that the TPA will remain in effect to the extent necessary for the trading partner or the Department to complete obligations involving EDI under the contract for dates of service when the contract was in effect.

(3) Trading Partner Agreement. To register as a trading partner with the Department, a provider, PHP, clinic, or allied agency must submit a signed TPA to the Department.

(4) Application for Authorization. In addition to the requirements of section (3) of this rule, a trading partner must submit an application for authorization to the Department. The application provides specific identification and legal authorization from the trading partner for an EDI submitter to conduct EDI transactions on behalf of a trading partner.

(5) Trading Partner Agents. A trading partner may use agents to facilitate the electronic transmission of data. If a trading partner will be using an agent as an EDI submitter, the application for authorization required under section (4) of this rule must identify and authorize an EDI submitter and must include the EDI certification signed by an EDI submitter before the Department may accept electronic submission from or send electronic transmission to an EDI submitter.

(6) EDI Registration. In addition to the requirements of section (3) of this rule, a trading partner must also submit its EDI registration form. This form requires the trading partner or its authorized EDI submitter to register an EDI submitter and the name and type of EDI transaction they are prepared to conduct. Signature of the trading partner or authorized EDI submitter is required on the EDI registration form. The registration form will also permit the trading partner to identify the individuals or EDI submitters who are authorized to submit or receive EDI registered transactions.

(7) Review and Acceptance Process. The Department will review the documentation provided to determine compliance with sections (1) through (6) of this rule. The information provided may be subject to verification by the Department. When the Department determines that the information complies with these rules, the Department will notify the trading partner and EDI submitter by email about any testing or other requirements applicable to place the registered transaction into a production environment.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0130
Trading Partner as EDI Submitter – EDI Transactions

(1) A trading partner may be an EDI submitter. Registered trading partners that also qualify as an EDI submitter may submit their own EDI transactions directly to the Department. A trading partner will be referred to as an EDI submitter when functioning in that capacity and will be required to comply with applicable EDI submitter rules, except as provided in section (3) of this rule.

(2) Authorization and Registration Designating Trading Partner as EDI Submitter. Before acting as an EDI submitter, a trading partner must designate in the application for application that they are an EDI submitter who is authorized to send and receive data transmissions in the performance of EDI transactions. A trading partner must complete the "Trading Partner Application for Authorization to Submit EDI Transactions" and the "EDI Submitter Information" required in the application. A trading partner must also submit the EDI registration form identifying them as an EDI submitter. A trading partner must notify the Department of any material changes in the information no less than ten days prior to the effective date of the change.

(3) EDI Submitter Certification Conditions. Where a trading partner is acting as its own EDI submitter, the trading partner is not required to submit the EDI submitter certification conditions in the application for authorization applicable to agents.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0140
Trading Partner Agents as EDI Submitters – EDI Transactions

(1) Responsibility for Agents. If a trading partner uses the services of an agent, including but not limited to an EDI submitter in any capacity in order to receive, transmit, store, or otherwise process data or data transmissions or perform related activities, a trading partner shall be fully responsible to the Department for the agent's acts.

(2) Notices Regarding EDI Submitter. Prior to the commencement of an EDI submitter's services, a trading partner must designate in the application for authorization the specific EDI submitters that are authorized to send and receive data transmissions in the performance of EDI transactions of a trading partner. A trading partner must complete the "Trading partner Authorization of EDI Submitter" and the "EDI Submitter Information" required in the application. A trading partner must also submit the EDI registration form identifying and providing information about an EDI submitter. A trading partner or authorized EDI submitter must notify the Department of any material changes in the EDI submitter authorization or information no less than five days prior to the effective date of the changes.

(3) EDI Submitter Authority. A trading partner must authorize the actions that an EDI submitter may take on behalf of a trading partner. The application for authorization permits a trading partner to authorize which decisions may only be made by a trading

partner and which decisions are authorized to be made by an EDI submitter. The EDI submitter information authorized in the application for authorization will be recorded by the Department in an EDI submitter profile. The Department may reject EDI transactions from an EDI submitter acting without authorization from a trading partner.

(4) EDI Submitter Certification Conditions. Each authorized EDI submitter acting as an agent of a trading partner must execute and comply with the EDI submitter certification conditions that are incorporated into the application for authorization. Failure to include the signed EDI submitter certification conditions with the application shall result in a denial of EDI submitter authorization by the Department. Failure of an EDI submitter to comply with the EDI submitter certification conditions may result in termination of EDI submitter registration for EDI transactions with the Department.

(5) EDI Submitters Responsibilities. In addition to the requirements of section (1) of this rule, a trading partner is responsible for ensuring that an EDI submitter makes no unauthorized changes in the data content of all data transmissions or the contents of an envelope, and that an EDI submitter will take all appropriate measures to maintain the timeliness, accuracy, truthfulness, confidentiality, security, and completeness of each data transmission. A trading partner is responsible for ensuring that its EDI submitters are specifically advised of, and will comply with, the terms of these rules and any TPA.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0150
Testing – EDI Transactions

(1) When a trading partner or authorized EDI submitter registers an EDI transaction with the Department, the Department may require testing before authorizing the transaction. Testing may include business-to-business testing. An EDI submitter must be able to demonstrate its capacity to send and receive each transaction type for which it has registered. The Department will reject any EDI transaction if an EDI submitter either refuses or fails to comply with the Department testing requirements.

(2) The Department may require EDI submitters to complete compliance testing at an EDI submitter's expense for each transaction type if either the Department or an EDI submitter has experienced a change to hardware or software applications by entering into business-to-business testing.

(3) When business-to-business testing is completed to the Department's satisfaction, the Department will notify an EDI submitter that it will register and accept the transactions in the production environment. This notification authorizes an EDI submitter to submit the registered EDI transactions to the Department for processing and response, as applicable. If there are any changes in the trading partner or EDI submitter authorization, profile data or EDI registration information on file with the Department, updated information must be submitted to the Department as required in OAR 407-120-0190.

(4) Testing will be conducted using secure electronic media communications methods.

(5) An EDI submitter may be required to re-test with the Department if the Department format changes or if the EDI submitter format changes.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0160
Conduct of Transactions – EDI Transactions

(1) EDI Submitter Obligations. An EDI submitter is responsible for the conduct of the EDI transactions registered on behalf of a trading partner, including the following:

(a) EDI Transmission Accuracy. An EDI submitter shall take reasonable care to ensure that data and data transmissions are timely, complete, accurate, and secure; and shall take reasonable precautions to prevent unauthorized access to the information system, the data transmission, or the contents of an envelope which is transmitted either to or from the Department. The Department will not correct or modify an incorrect transaction prior to processing. The transaction may be rejected and an EDI submitter notified of the rejection.

(b) Re-transmission of Indecipherable Transmissions. Where there is evidence that a data transmission is lost or indecipherable, the sending party must make best efforts to trace and re-transmit the original data transmission in a manner which allows it to be processed by the receiving party as soon as practicable.

(c) Cost of Equipment. An EDI submitter and the Department will pay for their own information system costs. An EDI submitter shall, at its own expense, obtain and maintain its own information system. An EDI submitter shall pay its own costs for all charges related to data transmission including, without limitation, charges for information system equipment, software and services, electronic mailbox maintenance, connect time, terminals, connections, telephones, modems, any applicable minimum use charges, and for translating, formatting, sending, and receiving communications over the electronic network to the electronic mailbox, if any, of the Department. The Department is not responsible for providing technical assistance in the processing of an EDI transaction.

(d) Back-up Files. EDI submitters must maintain adequate data archives and back-up files or other means sufficient to re-create a data transmission in the event that re-creation becomes necessary for any purpose, within timeframes required by state and federal law, or by contractual agreement. Data archives or back-up files shall be subject to these rules to the same extent as the original data transmission.

(e) Transmissions Format. Except as otherwise provided herein, EDI submitters must send and receive all data transmissions in the federally mandated format, or (if no federal standard has been promulgated) other formats as the Department designates.

(f) Testing. EDI submitters must, prior to the initial data transmission and throughout the term of a TPA, test and cooperate with the Department in the testing of information systems as the Department considers reasonably necessary to ensure the accuracy, timeliness, completeness, and confidentiality of each data transmission.

(2) Security and Confidentiality. To protect security and confidentiality of transmitted data, EDI submitters must comply with the following:

(a) Refrain from copying, reverse engineering, disclosing, publishing, distributing, or altering any data, data transmissions, or the contents of an envelope, except as necessary to comply with the terms of these rules or the TPA, or use the same for any purpose other than that which an EDI submitter was specifically given access and authorization by the Department or a trading partner;

(b) Refrain from obtaining access by any means to any data, data transmission, envelope, mailbox, or the Department's information system for any purpose other than that which an EDI submitter has received express authorization. If an EDI submitter receives data or data transmissions from the Department which clearly are not intended for an EDI submitter, an EDI submitter shall immediately notify the Department and make arrangements to return or re-transmit the data or data transmission to the Department. After re-transmission, an EDI submitter shall immediately delete the data contained in the data transmission from its information system;

(c) Install necessary security precautions to ensure the security of the information systems or records relating to the information systems of either the Department or an EDI submitter when the information system is not in active use by an EDI submitter;

(d) Protect and maintain the confidentiality of security access codes issued by the Department to an EDI submitter; and

(e) Provide special protection for security and other purposes, where appropriate, by means of authentication, encryption, the use of passwords, or other means. Unless otherwise provided in these rules, the recipient of a protected data transmission must at least use the same level of protection for any subsequent transmission of the original data transmission.

(3) Department Obligations. The Department shall:

(a) Make available to an EDI submitter, by electronic media, those types of data and data transmissions which an EDI submitter is authorized to receive.

(b) Inform an EDI submitter of acceptable formats in which data transmissions may be made and provide notification to an EDI submitter within reasonable time periods consistent with HIPAA transaction standards, if applicable, or at least 30 days prior by electronic notice of other changes in formats.

(c) Provide an EDI submitter with security access codes that will allow an EDI submitter access to the Department's information system. Security access codes are strictly confidential and EDI submitters must comply with all of the requirements of OAR 407-120-0170. The Department may change the designated security access codes at any time and manner as the Department, in its sole discretion, deems necessary. The release of security access codes shall be limited to authorized electronic data personnel of an EDI submitter and the Department with a need to know.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0165
Pharmacy Point of Sale Access

Pharmacy providers who electronically bill pharmaceutical claims must participate in and submit claims using the POS system, except as provided in OAR 410-121-0150.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0170
Confidentiality and Security

(1) Individually Identifiable Health Information. All providers, PHPs, and allied agencies are responsible for ensuring the confidentiality of individually identifiable health information, consistent with the requirements of the privacy statutes and regulations, and shall take reasonable action to prevent any unauthorized disclosure of confidential information by a provider, PHP, allied agency, or other agent. A provider, web portal submitter, trading partner, EDI submitter, or other agent must comply with any and all applicable privacy statutes and regulations relating to confidential information.

(2) General Requirements for Electronic Submitters. A provider (web portal submitter), trading partner (EDI submitter), or other agent must maintain adequate security procedures to prevent unauthorized access to data, data transmissions, security access codes, or the Department's information system, and must immediately notify the Department of all unauthorized attempts by any individual or entity to obtain access to or

otherwise tamper with the data, data transmissions, security access codes, or the Department's information system.

(3) Notice of Unauthorized Disclosures. All providers, PHPs, and allied agencies must promptly notify the Department of all unlawful or unauthorized disclosures of confidential information that come to its agents' attention, and shall cooperate with the Department if corrective action is required by the Department. The Department will promptly notify a provider, PHP, or allied agency of all unlawful or unauthorized disclosures of confidential information in relation to a provider, PHP, or allied agency that come to the Department's or its agents' attention, and will cooperate with a provider, PHP, or allied agency if corrective action is required.

(4) Wrongful use of the web portal, EDI systems, or the Department's network and information system, or wrongful use or disclosure of confidential information by a provider, allied agency, electronic submitters, or their agents may result in the immediate suspension or revocation of any access granted under these rules or other Department rules, at the sole discretion of the Department.

(5) A provider, allied agency, PHP, or electronic submitter must report to the Department's Information Security Office at dhsinfo.security@state.or.us and to the Department program contact individual, any privacy or security incidents that compromise, damage, or cause a loss of protection to confidential information, information assets, or the Department's network and security system. Reports must be made in the following manner:

(a) No later than five business days from the date on which a provider, allied agency, PHP, or electronic submitter becomes aware of the incident; and

(b) Provide the results of the incident assessment findings and resolution strategies no later than 30 business days after the report is due under section (4)(a).

(6) A provider, allied agency, PHP, or electronic submitter must comply with the Department's requests for corrective action concerning a privacy or security incident and with applicable laws requiring mitigation of harm caused by the unauthorized use or disclosure of confidential information.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0180
Record Retention and Audit

(1) Records Retention. A provider, web portal submitter, trading partner, and EDI submitter shall maintain, for a period of no less than seven years from the date of service, complete, accurate, and unaltered copies of all source documents associated with all data transmissions.

(2) EDI Trade Data Log. An EDI submitter must establish and maintain a trade data log that must record all data transmissions taking place between an EDI submitter and the Department during the term of a TPA. A trading partner and EDI submitter must take necessary and reasonable steps to ensure that the trade data log constitutes a current, truthful, accurate, complete, and unaltered record of all data transmissions between the parties and must be retained by each party for no less than 24 months following the date of the data transmission. The trade data log may be maintained on electronic media or other suitable means provided that, if necessary, the information may be timely retrieved and presented in readable form.

(3) Right to Audit. A provider must allow and require any web portal submitter to allow, and a trading partner must allow and require an EDI submitter or other agent to allow access to the Department, the Oregon Secretary of State, the Oregon Department of Justice Medicaid Fraud Unit, or its designees, and DHHS or its designees to audit relevant business records, source documents, data, data transmissions, trade data logs, or information systems of a provider and its web portal submitter, and a trading partner, and its agents, as necessary, to ensure compliance with these rules. A provider must allow and require its web portal submitter to allow, and a trading partner must allow and require an EDI submitter or other agent to allow the Department, or its designee, access to ensure that adequate security precautions have been made and are implemented to prevent unauthorized disclosure of any data, data transmissions, or other information.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0190
Material Changes

(1) Changes in Any Material Information – EDT Process. A trading partner must submit an updated TPA, application for authorization, or EDI registration form to the Department within ten business days of any material change in information. A material change includes but is not limited to mailing or email address change, contract number or contract status (termination, expiration, extension), identification of authorized individuals of a trading partner or EDI submitter, the addition or deletion of authorized transactions, or any other change that may affect the accuracy of or authority for an EDI transaction. The Department may act on data transmissions submitted by a trading partner and its EDI submitter based on information on file in the application for authorization and EDI registration forms until an updated form has been received and approved by the Department. A trading partner's signature or the signature of an authorized EDI submitter is required to ensure that an updated TPA, authorization, or EDI registration form is valid and authorized.

(2) Changes in Any Material Information – Web Portal Access. Providers must submit an updated web portal registration form to the Department within ten business days of any material changes in information. A material change includes but is not limited to mailing

or email address change, contract number or contract status (termination, suspension, expiration), identification of web portal submitter contact information, or any other change that may affect the accuracy of or authority for a DDE transaction. The Department is authorized to act on data transmissions submitted by a provider and its web portal submitter based on information on file in the web portal registration form until an updated form has been received and approved by the Department. A provider's signature or the signature of an authorized business representative is required to ensure that an updated web portal registration form is valid and authorized.

(3) Failure to submit a timely updated form may impact the ability of a data transaction to be processed without errors. Failure to submit a signed, updated form may result in the rejection of a data transmission.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065

407-120-0200
Department System Administration

(1) No individual or entity shall be registered to conduct a web portal or an EDI transaction with the Department except as authorized under these the rules. Eligibility and continued participation as a provider or web portal submitter in the conduct of DDE transactions, or as a trading partner or EDI submitter in the conduct of registered transactions, is conditioned on the execution and delivery of the documents required in these rules, the continued accuracy of that information consistent with OAR 407-120-0190, and compliance with a requirements of these rules. Data, including confidential information, governed by these rules may be used for purposes related to treatment, payment, and health care operations and for the administration of programs or services by the Department.

(2) In addition to the requirements of section (1) of this rule, in order to qualify as a trading partner:

(a) An individual or entity must be a Department provider, PHP, clinic, or allied agency pursuant to a current valid contract; and

(b) A provider, PHP, clinic, or allied agency must have submitted an executed TPA and all related documentation, including the application for authorization, that identifies and authorizes an EDI submitter.

(3) In addition to the requirements of section (1) of this rule, in order to qualify as an EDI submitter:

(a) A trading partner must have identified the individual or entity as an authorized EDI submitter in the application for authorization;

(b) If a trading partner identifies itself as an EDI submitter, the application for authorization must include the information required in the "Trading Partner Authorization of EDI Submitter" and the "EDI Submitter Information"; and

(c) If a trading partner uses an agent as an EDI submitter, the application for authorization must include the information described in section (3)(b) and the signed EDI submitter certification.

(4) The EDI registration process described in these rules provides the Department with essential profile information that the Department may use to confirm that a trading partner or EDI submitter is not otherwise excluded or disqualified from submitting EDI transactions to the Department.

(5) Nothing in these rules or a TPA prevents the Department from requesting additional information from a trading partner or an EDI submitter to determine their qualifications or eligibility for registration as a trading partner or EDI submitter.

(6) The Department shall deny a request for registration as a trading partner or for authorization of an EDI submitter or an EDI registration if it finds any of the following:

(a) A trading partner or EDI submitter has substantially failed to comply with the applicable administrative rules or laws;

(b) A trading partner or EDI submitter has been convicted of (or entered a plea of nolo contendre) a felony or misdemeanor related to a crime or violation of federal or state public assistance laws or privacy statutes or regulations;

(c) A trading partner or EDI submitter is excluded from participation in the Medicare program, as determined by the DHHS secretary; or

(d) A trading partner or EDI submitter fails to meet the qualifications as a trading partner or EDI submitter.

(7) Failure to comply with these rules, trading partner agreement, or EDI submitter certification or failure to provide accurate information on an application or certification may also result in sanctions and payment recovery pursuant to applicable Department program contracts or rules.

(8) For providers using the DDE submission system by the Department web portal, failure to comply with the terms of these rules, a web portal registration form, or failure to provide accurate information on the registration form may result in sanctions or payment recovery pursuant to the applicable Department program contracts or rules.

Stat. Auth.: ORS 409.050, 414.065
Stats. Implemented: ORS 414.065