

eHealth Exchange
OPP Glossary of Terms

Disclaimer: All other capitalized terms, if not defined within the OPP, shall have the same meaning as set forth in the DURSA.

**eHealth Exchange
OPP Glossary of Terms**

OPP	Term	Definition
7	Adverse Security Event	Adverse Security Event: shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content while in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant or Participant User or by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an “Adverse Security Event” under this Agreement does not include the following: (i) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User if— (I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and (II) such unencrypted Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or
1	Applicant	The entity or agency that submits an Application for Participation.
1	Application for Participation ("Application")	The document that serves as an application to participate in the eHealth Exchange.
1	Business Associate Agreement	The document that is attached to the eHealth Exchange Participant Agreement as Addendum 1. Anyone that provides a service to a HIPAA covered entity and has access to PHI as part of providing that service is a business associate of the covered entity. eHealth Exchange is a business associate of every eHealth Exchange Participant that uses the Hub and has entered into Business Associate Agreements with every eHealth Exchange Participant.
13	Controlled Unclassified Information	CUI) is information the Federal Government creates or possesses, or that an entity creates or possesses for or on behalf of the Federal Government, that a law, regulation, or Federal Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.
12	Customer(s)	An organization or an individual that purchases services from a Vendor Applicant and on whose behalf the Vendor Applicant exchanges information via the eHealth Exchange.
1-12	DURSA	Data Use and Reciprocal Support Agreement
13	DURSA	Shall mean “Restatement II of the Data Use and Reciprocal Support Agreement (DURSA),” Version Date: September 30, 2014 or Restatement III of the DURSA if Restatement III has been formally adopted before the Effective Date of this OPP.
1, 10, 12	eHealth Exchange	A network of Participants who share data in accordance with the DURSA.
3	eHealth Exchange Directory	Shall mean a directory of Participants that is used by Participants to find and Transact Message Content among Participants.

**eHealth Exchange
OPP Glossary of Terms**

OPP	Term	Definition
11	eHealth Exchange Hub	A centralized solution that operationalizes many of the Performance and Service Specifications that have been adopted by the eHealth Exchange. It employs shared infrastructure used to facilitate the transmission of messages for the eHealth Exchange network that may include, but is not limited to, gateway services, healthcare directory, and record locator services.
9	Federal Bridge Certificate Authority (FBCA)	The certification authority designed to create trust paths among individual agency PKIs by allowing discrete PKIs to trust digital certificates issued by other entities whose policies have been mapped and cross-certified with the FBCA
11	Hub Dashboard	An analytics dashboard built into the eHealth Exchange Hub solution that captures key operational metrics for Participants who initiate or respond over the Hub. The dashboard does not include data or metrics for point-to-point data exchange between Participants, as those transactions do not flow through the Hub and therefore the Hub and the Hub Dashboard have no knowledge of them.
8	Joinder Agreement	Shall mean the DURSA attachment each New Participant signs if they were not an original signatory to the DURSA.
1	Limited Production Period	A designated period of time after an organization has been issued their production digital credentials and been entered into the eHealth Exchange production directory, but is unable to begin transacting health information.
13	NIST	Shall mean the National Institute of Standards and Technology
2	Non-Federal Participants	Include all Participants that are not Federal agencies (e.g. health systems, state HIEs, regional HIEs, vendor networks).
9	Public Key Infrastructure (PKI)	The system employed by the eHealth Exchange to manage X.509 certificates used for the purposes of data encipherment, and message signature generation.
9	Responsible Disclosure	A practice developed by the Information Security community to ensure that identified vulnerabilities in security-related systems are resolved in a manner that protects the privacy and operational integrity of impacted systems until the vulnerability is remediated. A key component of this process is to only provide the vulnerability information on a need to know basis.
9	REST	An acronym for Representational State Transfer which is a method of information exchange that uses a web-browser-like approach to contact message content. This method is used by the HL7 FHIR® standard.
9	Secure Environment	In the context of this OPP, a secure environment is defined as a single computer, in a data center with appropriate physical and software access controls to prevent inappropriate access by unauthorized people or systems. A secure environment also optionally includes a high availability cluster of computers designed to mimic the cryptographic behavior of a single system, and it also includes a disaster response data center operated to closely mimic the behavior of the primary data center.
3	Service Change	Shall mean changes in regard to Transaction Patterns and suspensions and terminations of a Participant.
9	SOAP	A method of transacting message content exchange using XML. This method is used by the eHealth Exchange Patient Discovery, Messaging Platform, Access Consent Policies, and other specifications.
9	Subscriber	A Subscriber refers to the person a Participant has officially authorized to receive and accept responsibility for the secure use and management of the Participant's x.509 public certificate and its associated keys. This individual must be able to enter into binding legal agreements on behalf of the Participant, and must be identity proofed, in person, by a licensed Notary at least every 24 months. The eHealth Exchange suggests, but does not require this individual be an Information Technology professional with sufficient technical and security knowledge in order to successfully oversee installation of the eHealth Exchange x.509 certificate.
1	Third Party Technology	Technology solutions, applications, interfaces, software, platforms, clearinghouses and other IT resources utilized by Participants to facilitate exchange.

**eHealth Exchange
OPP Glossary of Terms**

OPP	Term	Definition
3	Transaction Pattern	Shall mean a type of information exchange service(s) enabled by the Specifications. The Validation Plan will identify the Transaction Pattern(s) and the Specifications required to implement each Transaction Pattern. The Transaction Patterns may be amended from time to time through amendment of the Specifications and the Operating Policies and
9	Transport Layer Security (TLS)	A method the eHealth Exchange uses to create secure (private, intact, and authentic) communications channels between Participants.
12	Vendor Applicant	The vendor entity that submits an Application for Participation