## Application for Participation in the eHealth Exchange

Form Revised 09/05/2024

INSTRUCTIONS:

**Please complete and e-mail the following information to** [administrator@ehealthexchange.org](mailto:administrator@ehealthexchange.org)

**All documents are available at** available at <https://ehealthexchange.org/onboarding/how-to-apply>

1. A complete and signed Application for Participation

* The signed Joinder Agreement (Attachment 7 of Data Use and Reciprocal Support Agreement (DURSA) Populate ‘Contacts for Notices’ (Attachment 4 of the DURSA and provide a Primary Contact (you may also provide an Alternative Contact)
* Please do not sign DURSA pages 35 of 50 or page 50 of 50 as you are signing a Restatement of the DURSA and are not a signatory of the original DURSA

1. The signed eHealth Exchange Participation Agreement.

* Populate your organization’s name,
* Complete the name, address and contact information of your Designated Representative on page 3.
* Sign and date the Addendum 1, Business Associate Agreement (BAA)

1. The signed eHealth Exchange Testing Agreement
2. The completed Contact List(each type of resource should be identified to facilitate effective communication from eHealth Exchange)

This document serves as an application to participate in the eHealth Exchange. Those who participate in this electronic exchange of health information are known as “Participants.”

Organizations that wish to be considered for “Participant” status should complete and submit this Application for Participation. The eHealth Exchange Coordinating Committee (“Coordinating Committee”) is responsible for reviewing and acting upon Applications for Participation. The Participants have granted the Coordinating Committee this responsibility in Section 4.03 of the DURSA.

To assist the Coordinating Committee in fulfilling its responsibility in a consistent and effective manner, the Participants have adopted an Operating Policy and Procedure for Review and Disposition of Applications (www,ehealthexchange.org ). The Coordinating Committee will review the Applicant’s Application in accordance with this Operating Policy and Procedure.

All information in this Application for Participation will be used by the Coordinating Committee to determine whether the Applicant meets the eligibility requirements for participation.

If the Coordinating Committee determines that the Applicant meets the eligibility requirements for participation and has successfully completed all applicable technical testing, the Coordinating Committee will conditionally accept the Applicant as a Participant.

The Applicant becomes a Participant only when: (i) the Applicant’s system is operational, in production, and ready to exchange information with other Participants in production; (ii) the Applicant has installed the production Digital Credentials (i.e., production X.509 digital certificate), if applicable; and (iii) the DURSA Joinder Agreement has been countersigned by the Coordinating Committee and a copy sent back to the Applicant. Until all of the foregoing have occurred, the Applicant may not publicly refer to itself as a “Participant.”

**NOTE: The DURSA Joinder Agreement and Participation Agreement WILL NOT be countersigned by the Coordinating Committee until your organization has installed digital security certificates in your production environment and eHealth Exchange staff has entered your organizations routing endpoints in the eHealth Exchange directory.**

**This document is submitted this, the \_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_, 20\_\_, to the eHealth Exchange Coordinating Committee by the organization listed below (“Applicant”) to become a Participant in the eHealth Exchange.**

Part I: Basic Applicant Information

|  |  |
| --- | --- |
| **Organization Name:** |  |
| **Address:** |  |
| **Web Site:** |  |
| **Phone Number:** |  |
| **EIN:** |  |

Part II: Applicant Information

|  |
| --- |
| 1. **Organization Type and Size** |

|  |
| --- |
| Is your organization a Governmental Participant applicant?  Yes  No  Note: The DURSA defines Governmental participants as local, state or federal agencies |
|  |
| |  |  | | --- | --- | | Organization Type | Description | | Provider Organization  Hospital Organization  Ambulatory Provider Group  Provider Collaborative  Post-Acute Organization | An organization that delivers care.  An organization that owns and operates a network for one or more healthcare facilities, often providing many different types of inpatient and outpatient services. This includes Academic, Community, Children's, Behavioral health, and specialty hospitals.  Care provided on an outpatient basis, including physician groups, clinics, ambulatory surgery centers, dialysis, and urgent care centers.  Independent but aligned physicians, hospitals or health systems that have a legal partnership agreement.  Skilled nursing facilities, inpatient rehabilitation, custodial, home health, hospice organizations without being a subsidiary of a hospital organization. | | Health Information Network | Health information network (HIN) or electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient’s vital medical information electronically. | | Public Health | All public, private, and voluntary entities that contribute to the delivery of essential public health services within a jurisdiction. | | Payer | Organizations such as health plan providers, insurers, Medicare, and Medicaid, Pharmacy Benefits Management, and third-party administrators that set service rates, process claims, and collect payments, and pay provider claims. | | Individual Access | Organizations that provide software allowing consumers to aggregate and share their health information. | | Research and Data Management | Organizations that use clinical data from multiple sources for research including disease registries, clinical trials, etc. | | Vendor or Service Provider | Organizations that sell software and/or services or acts as a conduit (go between) for services. Includes electronic health and medical record systems, e-prescribing solutions, identity proofing, etc. | |

|  |
| --- |
| Applicant’s Adjusted or Net Patient Revenue: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_   * Please round down to the nearest million. * Governmental and Non-patient revenue generating organizations should report annual operating expenses instead. * This information is used to determine the annual participation fee and will be updated annually |
| 1. **Applicant’s Size:**  |  |  |  | | --- | --- | --- | |  | Types | Total # | |  | # of Hospitals |  | |  | # of Medical Groups (e.g. ambulatory / physician practices, post-acute settings, dialysis centers, etc. |  | |  | Other (please describe) |  | |  | | | |  | | | | Please identify the states & US territories where your organization maintains a physical presence and patient data will be exchanged: | | | |
| 1. **Technology Partner:** indicate the technology solution(s) that Applicant plans to use for participation in the eHealth Exchange.  |  | | --- | | Vendor: | | Product Name: | | Version #: | | Additional information: | | |

Part III. DURSA Flow-Down Provisions

The Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party, trust agreement that is executed by all Participants in the eHealth Exchange. Please ensure that you have reviewed the DURSA in its entirety and that your organization has implemented measures needed to comply with its provisions. Your organization must have enforceable mechanisms to assure that other participating organizations or users with access to your eHealth Exchange connection similarly comply.The questions outlined below will assist the Coordinating Committee assess the flow-down mechanisms currently implemented by your organization, as well as your plans to implement those not currently in place.

We understand your organization may need to create or modify legal agreements and/or policies and procedures to obligate your participating organizations and users abide by the terms of the DURSA.Any changes must be implemented prior to the eHealth Exchange Go-Live Date. Additional guidance for each provision is provided in Attachment #1.

|  |
| --- |
| 1. **Does your organization use a third-party intermediary or health information exchange service provider to conduct the exchange of health information on your behalf, pursuant to Section 15.05 of the DURSA?**   Yes. This organization uses a third-party intermediary or health information exchange service provider who facilitates the exchange of health information on our behalf.  Please provide a 1-2 sentence statement for each question 5a – 5d to describe how you are enforcing compliance so that your third-party intermediary or health information exchange service provider complies with the terms of the DURSA. If you need to modify your contracts or business agreements to comply, please describe what changes are needed (e.g., requiring your IT vendor to cooperate with a DURSA issue) and how you plan to effectuate those changes (e.g., amending the IT vendor agreement).  No. This organization does not use a third-party intermediary or health information exchange service provider who facilitates the exchange of health information on our behalf. **(Proceed to Part V.) (If your organization uses Epic, Cerner, or another EHR check this option.)** |
| 4a. Does your organization have contracts or business agreements in place that assure that 3rd party intermediaries or health information exchange service providers comply with Applicable Law? If yes, please describe. |
| 4b. Does your organization have contracts or business agreements in place that assure that that 3rd party intermediaries or health information exchange service providers protect the privacy and security of any Message Content to which it they access? If yes, please describe. |
| 4c. Does your organization have contracts or business agreements in place that ensure 3rd party intermediaries or health information exchange service providers notify your organization as soon as reasonably practicable after determining that suspected or actual Adverse Security Event has occurred? If yes, please describe. |
| 4d. Does your organization have contracts or business agreements in place that ensure 3rd party intermediaries or health information exchange service providers reasonably cooperate with the other Participants regarding issues related to the DURSA, under the direction of your organization? If yes, please describe. |
|  |

|  |
| --- |
| 1. **Does your organization have enforceable agreements or policies and procedures in place to obligate your participating organizations or users to comply with each of the below provisions, pursuant to Section 15.04 of the DURSA?**   **This section requires an answer to each question.**  This question is intended to clarify how your organization has implemented certain obligations in Section 15.04 of the DURSA. eHealth Exchange Participants must carry through DURSA obligations to participating organizations or users who will use your organization’s eHealth Exchange connection. Any organization or individual who is able to access and either initiate or receive messages through your eHealth Exchange connection is held to the same standards in the DURSA in order to maintain a chain of trust in the Exchange.  Please provide a 1-2 sentence statement for each of the following to describe how you are enforcing compliance with your other participating organizations or users.  If you need to modify your policies/procedures/agreements to comply with these provisions, please indicate what changes are needed (e.g., requiring users to cooperate with a DURSA issue) and how you plan to effectuate those changes (e.g., adopting a new policy and procedure). |
| 5a. Does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or users comply with Applicable Law? If yes, please describe. |
| 5b. Does your organization have policies, procedures, and/or enforceable agreements in place that ensure your participating organizations and/or your users will reasonably cooperate with your organization regarding any issues related to the DURSA? If yes, please describe. |
| 5c. Does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or your users will request, retrieve, and send data only for a Permitted Purpose defined in the DURSA (which may be more restrictive than HIPAA)? If yes, please describe. |
| 5d. Does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or your users only use data received via the eHealth Exchange in accordance with applicable law and your data retention policies. If yes, please describe. |
| 5e. Does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or your users will report **suspected** and **confirmed** Adverse Security Events to your organization in order for you to fulfill your obligations in responding to the Adverse Security Event notification requirements in the DURSA (Refer to DURSA Section 14.04). A DURSA Adverse Security Event involves an incident that compromises the transmission of data via your eHealth Exchange connection (Refer to DURSA Section 1 (d)). If yes, please describe. |
| 5f. Does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or your users will not disclose any passwords, digital security certificates issued by the eHealth Exchange technical support group, or any other security measures issued to that participating organization enabling connectivity to the eHealth Exchange and / or user by your organization? If yes, please describe. |
| 5g. If your organization permits individuals/consumers to retrieve their own personal data via eHealth Exchange, does your organization have policies/procedures/enforceable agreements in place that ensure your participating organizations and/or your users comply with the Consumer Identity Proofing Performance Specification (Identity Assurance Level 2 or 3 as described in NIST Special Publication 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>)?  Please note this does not apply to most Applicants. |

By checking this box, if the Applicant needs to create new or make modifications to policies/procedures, contracts, or business agreements, etc., in order to comply with the DURSA flow-down provisions, the Applicant attests that these requirements will be implemented prior to the Go-Live Date and understands such attestation will be verified by eHealth Exchange staff.

|  |
| --- |
| 1. Please describe your organization’s product or service (e.g., EHR, care coordination platform, etc.) |
| 1. Please explain if and how your organization’s use case meets the definition of Treatment ([45 CFR 164.506](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html)), and if and how your organization intends to use the patient data it receives from eHealth Exchange to support the use case. In your answer, please describe your primary Use Case and any secondary Use Case or Cases. |
| 1. Is your organization a [Covered Entity](https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html) as defined by [HIPAA? If so, what type of Covered Entity is it?](https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996)    1. Health Care Provider ([HIPAA definition](https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996))    2. Other (please specify)    3. No (see question 4) |
| 1. If your organization is not a Health Care Provider, is it a [Business Associate](https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html) of Health Care Providers (*i.e.*, does your organization have Business Associate Agreements in place allowing it to act on behalf of those Health Care Providers)? Y/N |
| 1. Will licensed providers (*e.g.*, MDs, DOs, NPs, etc.) be the primary users of the requested PHI? Y/N If no, required to answer #6 below. |
| 1. If licensed providers will NOT be the primary end users of the requested PHI, please explain who will have access to data obtained through eHealth Exchange (*i.e.*, who will be the end users of PHI being requested). What will end users do with the data to impact the treatment of patients? Are those end users operating on behalf of, or in conjunction with a licensed provider (*e.g.*, M.D., D.O., N.P., etc.)? |
| 1. Is there an existing or anticipated [direct care relationship](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/standards-privacy-individually-identifiable-health-information/index.html#:~:text=A%20provider%20with%20a%20direct,and%2C%20therefore%2C%20is%20permissible.) between licensed providers (either your organization’s providers or your customer’s provider(s)) and the patients for whom data is being requested? |
| 1. Will the data requested be utilized in individually [anticipated encounter](https://www.healthit.gov/buzz-blog/privacy-and-security/real-hipaa-care-coordination-care-planning-case-management-examples)s or care decisions (inclusive of Care Coordination pursuant to [45 CFR 164.506I(2)](http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-506.pdf))? |
| 1. Is your organization able to support network bi-directionality obligations? (*i.e.,* is it (or its customers) able to generate unique clinical data (such as notes, observations, and reports) to share back with the networks via its connection with eHealth Exchange participants? Please summarize the type and scope of data your organization will provide back to eHealth Exchange. The DURSA requires Participants requesting data for Treatment purposes to share data with other Participants and requesting data for Treatment purposes. |
| 1. If your organization intends for any of its customers to use data retrieve data via eHealth Exchange, can your organization identify the initiating customer in its messages’ SAML or FHIR headers when your organization’s customers initiate requests for data? Y/N |
| 1. If your organization indicated “no” to question 10 and/or 11 please explain what will trigger queries (i.e., requests for data) and when the data received will be utilized? |
| 1. Does your organization have data sources to which you can respond with data when your organization matches the patient and you have data? Y/N Explain if your organization answered no. |
| 1. If your organization is a vendor or service provider, please provide answers to questions 1-12 for all of its existing customers, and then as you add new customers, and submit responses pertaining to these customers for eHealth Exchange staff consideration before your customers initiate and respond to eHealth Exchange queries. |

|  |
| --- |
| **Definitions** |
| Health care provider  *Health care provider* means a provider of services (as defined in section 1861 of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. |
| Purpose of use (if for Treatment)  *Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. Treatment explicitly excludes services defined in payment and other healthcare operations. |
| Care Coordination  Any activity that helps ensure that the patient's needs and preferences for health services and information sharing across people, functions, and sites are met over time. Care coordination MUST be provided as part of Treatment. |

Part IV: Technical Eligibility Requirements

**Select all the eHealth Exchange Use Cases and corresponding eHealth Exchange Technical Specifications Applicant will initially support in production via the eHealth Exchange.**

*Please note that after being accepted as a Participant, Participants are encouraged to implement additional Transaction Patterns (Use Cases and technical Specifications) in accordance with Operating Policy and Procedure #3: Participation Changes, Suspension and Termination (*[*https://ehealthexchange.org/policies/*](https://ehealthexchange.org/policies/)*).*

**Pull Data (Query and Retrieve):**

Query and Retrieve comprehensive clinical documents

Transported via IHE profiles (XCPD & XCA) [most common response]

Transported via FHIR

Retrieve comprehensive clinical documents (HL7 C-CDAs, CCDs, CDAs) [most common response]

Retrieve large DICOM images

Retrieve only specific data categories via HL7 FHIR (e.g., medications only or lab results only)

For Treatment, Healthcare Operations, and Payment purposes. [most common response]

With specific patient Authorization

for Social Security Administration benefit determinations [common response]

for Life Insurance policy determinations

for Personal Health Record population

for Research

for Other Purposes (please describe)

Comments:

**Push Data:**

For Electronic Case Reporting (syndromic surveillance) to Association of Public Health Laboratories to route to appropriate public health authorities [common response]

Push via ITI-41 (C-CDAs pushed via XDR, XDS, or XCDR)

Push via Direct Securing Messaging

* eHealth Exchange offers the trust framework to support Direct Secure Message exchange with other eHealth Exchange Participants, as well as the technical routing services via APHL (Association of Public Health Laboratories)
* eHealth Exchange does not provide any HISP (Direct platform) services

To populate regional HIEs’ longitudinal patient records

To push immunization administration (not to registries)

To push for other reasons. Please specify\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Comments:

Part V: Enhanced Connectivity Agreements

Section 4.03(m) of the DURSA grants the Coordinating Committee authority to enter into agreements to broaden access to data through enhanced connectivity across platforms and networks (herein referred to as an “Enhanced Connection(s)”). The Coordinating Committee has entered into such agreements for the Enhanced Connection(s) listed and briefly described in this Part V. Pursuant to Section 12.05 of the DURSA, an eHealth Exchange Participant may choose to **opt-out** of participation in any/all such Enhanced Connection(s), for any reason, by providing written notification of the decision to opt out. Furthermore, a Participant may reverse its decision at any time by providing such decision to the Coordinating Committee in writing.

The following Enhanced Connections are currently made available through the eHealth Exchange. If your application is approved, your organization will participant in the exchange of information with the Enhanced Connections listed below **UNLESS you affirmatively opt-out of such participation**.

Organizations that choose to opt-out of Carequality and/or TEFCA exchange, may opt-in at a later date for no additional fees.

**Car*e*quality**

Carequality is a framework with a library of technical and policy agreements, plus a governing structure, that enables independent health data networks to exchange patient data.  The Carequality framework is made up of 35+ networks, such as the AthenaNet network, the eClinicalWorks network, Common Well, and many other eHealth Exchange peer networks. This Enhanced Connection provides an integrated solution for Participants to exchange patient information with healthcare organizations that are not part of the eHealth Exchange but that exchange information within Carequality-enabled networks.

**My organization wishes to opt-out of exchanging with Carequality-enabled networks via the eHealth Exchange:**

**Yes**

**No** – My organization does **not** wish to opt-out. This means that your organization agrees to comply with the [Carequality Connection Terms](https://carequality.org/resources/). Your initials here evidence your agreement. Initial: \_\_\_\_\_\_\_

**TEFCA**

TEFCA is a federally-endorsed a framework designed to scale Electronic Health Information exchange nationwide and help ensure that health care providers, Health Information Networks, health plans, individuals and many more stakeholders have secure access to their electronic health information when and where it is needed. This Enhanced Connection provides an integrated solution for Participants to exchange patient information with healthcare organizations that are not part of the eHealth Exchange but that exchange information within other Qualified Health Information Networks within the TEFCA framework.

**My organization wishes to opt-out of exchanging with TEFCA via the eHealth Exchange:**

**Yes**

**No** – My organization does **not** wish to opt-out. This means that your organization agrees to comply with the [Participant/Subparticipant Terms of Participation, eHealth Exchange TEFCA Terms and Conditions, SOPs and Protocols, and technical requirements](https://ehealthexchange.org/what-we-do/tefca-and-ehealth-exchange/) for exchanging data via TEFCA. Your initials here evidence your agreement. Initial: \_\_\_\_\_\_\_

Part VI: Invoicing and Payment Information:

1. Do your accounts payable department have requirements to process invoices beyond receiving the invoice and W-9? If yes, please provide those requirements below:

­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Purchase Order (PO) – if a PO is required who at your organization will provide this to eHealth Exchange?

­­­­­­­­­­­­­­­­­

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Additional forms – If any forms are required to be completed, who can eHealth Exchange request these from now?

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Vendor Registration Set up – If eHealth Exchange needs to complete a Vendor Registration who can we request this from now?

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Many times the accounts payable department requests the countersigned Participation Agreement/BAA, DURSA, and Testing Agreements to process payment, who at your organization should be added to the email when eHealth Exchange countersigns each one?

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Part VII: Attestations

As an Applicant to the eHealth Exchange, please attest (by checking each box) that the following statements are true and accurate.

Applicant is a valid business in good standing or a governmental agency, operating in the United States;

Applicant meets all solvency and financial responsibility requirements imposed on the Applicant be applicable statutes and regulatory authorities;

Applicant is an organization or agency that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations;

Applicant has the organizational infrastructure and legal authority (through statutes, regulations, organizational agreements, contracts or binding policies) to comply with the obligations in the DURSA and to require its Participant Users to comply with applicable requirements of the DURSA;

Applicant intends to Transact information with other Participants for a Permitted Purpose;

Applicant has sufficient financial, technical and operational resources to support the testing and operation of transactions among Participants;

In the event that resource issues arise, Applicant agrees to communicate and coordinate with the eHealth Exchange Coordinating Committee regarding Applicant’s situation.

Applicant is not aware of any information that would preclude the Applicant from fully complying with the provisions of the DURSA;

Along with this Application, Applicant is submitting:

1. The signed DURSA Joinder Agreement (Attachment 7 of the DURSA) with Attachment 4 – Contacts for Notice) populated. Please do not sign DURSA page 35 of 50 or page 50 of 50.
2. The signed eHealth Exchange Participation Agreement (version dated May 2019). Do not forget to populate your organization’s name and to sign and date the Addendum 1 Business Associate Agreement.
3. The signed eHealth Exchange Testing Agreement
4. The Contact List

The information contained in this Application for Participation is true and accurate. Applicant will notify the Coordinating Committee if the information contained herein materially changes.

|  |  |  |
| --- | --- | --- |
| **For: [Enter Your Organization’s Name]** | |  |
|  |  |  |  |
| Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |
| Signature: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |
| Printed Name: | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |  |
| Title: | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |  |

**Attachment 1 - Onboarding Resources and DURSA Guidance**

**Onboarding Resources**

The resources below are available to assist you in completing the application package. These resources can be found on the Onboarding page of the eHealth Exchange website at [www.ehealthexchange.com:](http://www.ehealthexchange.com:)

1. Onboarding Overview – This presentation provides an overview of the onboarding process;
2. DURSA Policy Assumptions – These slides highlight the DURSA including the overall context and DURSA provisions;
3. eHealth Exchange Participant Testing Program Process – This document provides a step-by-step overview of the onboarding and testing process.

**DURSA Flow-Down Provision Guidance**

The DURSA requires that your organization, your users, your participating organizations, and your technology partners, if there are any, to comply with the DURSA Provisions. The following represents additional clarifications to help applicants answer question #4 on the application.

The Coordinating Committee is looking for a 1-2 sentence statement for each provision that explains how your organization obligates its participating organizations and/or users who will access your organization’s eHealth Exchange connection to comply with the applicable DURSA provisions. The following questions/guidelines below each provision should be used to help you to answer Question #4 on the application.

1. **Users must comply with all applicable law**
   * How does your organization obligate its users (or participants if you are an HIE/HIO) to comply with applicable law?  For example:
     + Does your organization have policies (e.g., Human Resources, etc.) or employment agreements that obligate employees or contract staff to comply with Applicable Law?
     + Do your contracts/arrangements with medical staff obligate them to comply with Applicable Law?
2. **Users must reasonably cooperate with your organization regarding any issues related to the DURSA**
   * Your legal counsel should review the DURSA carefully to understand your organization’s obligations in the DURSA and to assure you have appropriately implemented the applicable “flow-down” provisions to your users or other participating organizations.   For example:
     + Under 12.02, a Participant’s users must comply with terms of DURSA, including use, confidentiality, privacy, and security of Message Content.  Participant shall appropriately discipline users who fail to act accordingly.
     + Under 15.04, a Participant’s users must cooperate with reporting and responding to DURSA Adverse Security Events (which are defined differently from HIPAA breaches)
   * How will your organization obligate its users to meet specific provisions in the DURSA, such as Sections 5.01, 12.02, 13, etc.?
     + For example, do your organization’s policies (e.g., Human Resources, etc.) or employment agreements obligate employees or contract staff to cooperate with your organization in complying with Applicable Law and the organization’s obligations under the DURSA?
     + Do your organization’s contracts / arrangements with medical staff obligate them to cooperate with your organization so it can satisfy its obligations under Applicable Law and the DURSA?
3. **Only transmit data for permitted purposes defined in the DURSA, which may be more narrow than what is permitted in HIPAA**

* Participants may NOT use eHealth Exchange connectivity for any purpose EXCEPT those specified in the definition of Permitted Purposes in the DURSA. Does your organization have a policy consistent with the DURSA to ensure that users will only request data or submit data via the eHealth Exchange connection for purposes outlined in the Permitted Purposes definition?
* The permitted purposes in the DURSA may be more stringent than HIPAA.
  + Treatment - Treatment of the individual who is the subject of the Message.  Not for treatment purposes for other patients or for general treatment purposes by the Health Care Provider.
  + Payment activities of a Health Care Provider as they relate to the individual who is the subject of the Message.
    - For example, this could be in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan.
  + Limited Healthcare Operations
    - Healthcare operations of the Covered Entity submitting the data or when another organization submits the data on a Covered Entity’s behalf.
    - Healthcare operations of a Health Care Provider who receives the message and has an established Treatment relationship with the individual who is the subject of the Message.
  + Public Health Activities and Reporting
  + Any Purpose to Demonstrate Meaningful Use
  + Uses and Disclosures Pursuant to an Authorization
  + Transaction of Message Content in support of an individual’s: (i) right to access his/her health information or (ii) right to direct with whom his/her information can be shared and/or where such information should be sent.

1. **Only use data received from your Organization or other Exchange Participants in accordance with the terms and conditions of the DURSA**

* The ultimate recipient of records received (i.e., a copy of another Participant’s records), may incorporate that data into its records and retain that information in accordance with Applicable Law and the recipient’s record retention policies and procedures.

1. **Appropriately report Adverse Security Events (as defined in the DURSA) within the timeframes specified in the DURSA.**

* The reportable Adverse Security Events in the DURSA are different than those that must be reported for HIPAA.   Adverse Security Events are defined very narrowly to apply to inappropriate access/use/disclosure as it relates to the transmission of data with other eHealth Exchange Participants. For details, refer to the DURSA definition of Adverse Security Events.
* Participants are required to notify the eHealth Exchange Coordinating Committee and other impacted Participants of DURSA Adverse Security Events within specific timeframes:
  + Within 1 hour of ***suspected*** Adverse Security Event, participants are required to notify the CC and impacted federal Participants (5 business days for non-federal Participants)
  + Within 24 hours of ***confirmed*** Adverse Security Event, notify the Coordinating Committee, take steps to mitigate the Adverse Security Event, and implement corrective action plans to prevent such Adverse Security Events in the future

*NOTE: The difference between the 1 hour/5 business day and 24 hour notifications will depend on how long it takes your organization to complete the analysis required to confirm that there was an Adverse Security Event.  The 24 hour/5 business day notification begins once this confirmation has been made.*

1. **Refrain from disclosing to anyone any passwords or other tokens issued by your Organization, as well as the digital certificates issued for the eHealth Exchange.**
   * Participants must have a policy or procedure that requires users/participants to protect any passwords and any other security tokens that grant system access or enable the exchange of data with other eHealth Exchange participants.